InRouter 600 Series User's Manual

First Edition, August, 2011

© 2011 InHand Networks, All rights reserved.
Republication without permission is prohibited.

InRouter 600 Series User's Manual

Copyright Notice
Copyright © 2011 InHand Networks
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

InHand is a registered trademark of InHand Networks. Other registered marks cited in this manual represented their respective companies.

Disclaimer

Information in this document is subject to change without notice and does not represent an obligation on the part of InHand Networks.

This user manual may include intentional technical or typographical errors. Changes are periodically made to the manual to correct such errors, and these changes are not informed in new editions.

Technical Support Contact Information

InHand Networks, China
Tel: +86-010-64391099
Fax: +86-010-84170089
Email: support@inhandnetworks.com

I

Introduction to InRouter 601

- Overview
- Package Checklist
- Product Features & Specifications
- Product Models

1.1 Overview

InRouter600 series are desktop industrial grade cellular router which set the traditional router functions and the advantages of 3G networks. Products take industrial grade chip design, pre-3G communication module access global 2.5G and 3G networks in a high speed, support routine protocols like PPP, NAT, RIP, GRE, VRRP.

InRouter600 series cellular routers are low power consumption, large range operating temperature from -25℃ to 70℃, small size, light weight, easy to use in harsh industrial circumstance. InRouter601 is ideal for industrial applications choice.

InRouter 600 series products support VPN (IPSec/PPTP/ L2TP/GRE/SSL VPN), which create high-security links between remote equipment and customer's center. Application data in a secure IPSec tunnel transmission, preventing data be thieved and tampered. It provides advanced security for network application.

In addition, InRouter600 series products support the Device Manager remote device manage platform, which realizes remote operation including remote control, remote monitor, parameters configure, firmware upgrade, log/alarm management, information statistics/display, batch configuration/update and etc.

Important Safety Information

This product is not intended for use in the following circumstances

- Area(s) where radio transmission equipment (such as cell phone) are not permitted.
- Hospitals, health care facilities and area(s) where cell phones are restricted by law.
- Gas stations, fuel storage and places where chemical are stored.
- Chemical plants or places with potential explosion hazard.
- Any metal surface that may weaken the radio signal level.

RF safety distance

- For GPRS router, the compliance boundary distance is r=0.26m for GSM 900MHz and r=0.13m for DCS 1800 MHz.
- For HSUPA router, the compliance boundary distance is r=0.26m for GSM 900MHz and
- r=0.13m for DCS 1800 MHz, r=.0.094 for WCDMA 900MHz, r=0.063 for WCDMA 2100MHz.

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

WEEE Notice

The Directive on Waste Electrical and Electronic Equipment (WEEE), which entered into force as European law on 13th February 2003, resulted in a major change in the treatment of electrical equipment at end-of-life.
The purpose of this Directive is, as a first priority, the prevention of WEEE, and in addition, to promote the reuse, recycling and other forms of recovery of such wastes so as to reduce disposal.

The WEEE logo (shown at the left) on the product or on its box indicates that this product must not be disposed of or dumped with your other household waste. You are liable to dispose of all your electronic or electrical waste equipment by relocating over to the specified collection point for recycling of such hazardous waste. Isolated collection and proper recovery of your electronic and electrical waste equipment at the time of disposal will allow us to help conserving natural resources. Moreover, proper recycling of the electronic and electrical waste equipment will ensure safety of human health and environment.

For more information about electronic and electrical waste equipment disposal, recovery, and collection points, please contact your local city centre, household waste disposal service, shop from where you purchased the equipment, or manufacturer of the equipment.

1.2 Package Checklist

We put each In Router 601 cellular router in a box with standard accessories. Additionally, there're optional accessories can be ordered. When you receive our package, please check carefully, and if there're items missing or appearing to be damaged, please contact with your InHand Networks sales representative.

Items in package include:

Standard Accessories:

Accessories	Description
InRouter 600 Serials Wireless Router	1
Cable	1 Cross line,CAT-5,1.5M
Document and Software CD	1
Antenna	5m Cellular Antenna
Power Supply	
	Power Adapter, 100-265V AC in, 12V DC out

Optional Antennas:

Picture	Type	Description
	GSM/GPRS Cellular Antennas	GPRS Quad-band (included in IR7xxGS55)
	UMTS/HSDPA/WCDMA Cellular Antennas	WCDMA Quad-band (included in IR7xxWH01)
	Anti-thief antenna	WCDMA Quad-band (Optional for IR7xxWH01)
	Stick antenna	WCDMA Quad-band (Optional for IR7xxWH01)
	Anti-thief antenna	WCDMA Quad-band (Optional for IR7xxWH01)

1.3 Product Features

1.3.1 Interface

WAN

Cellular WAN:

Band Options:

HSUPA /HSDPA/WCDMA
850/900/1900/2100MHz
GSM/GPRS/EDGE
850/900/1800/1900MHz

Ethernet WAN:

Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX

Magnetic Isolation Protection: 1.5 KV built-in

LAN

IR601/611

Number of Ports: 1

Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX

Magnetic Isolation Protection: 1.5 KV built-in

Serial

A. Serial Type: RS232/485
B. Serial form: COM, DB-9
C. Data bit: 5/6/7/8
D. Stop bit: 1/2
E. Check bit: N/O/D
F. Baud rate: 1,200bit/s~ 115,200bit/s

SIM Interface

SIM Control: 3 V

1.3.2 Functions

PPP

Supported VPDN/APN, fast access to virtual private dial-up network (VPDN) provided by mobile operator, ensure high-security data transmission.

Support CHAP/PAP/MS-CHAP/MS-CHAP V2 authorization

Support Connection Detection, auto-recovery, auto-link, ensure reliable communication.

Support On-demand connection, SMS Activity

Dynamic IP

Support DHCP, applied as Server/Client

Dynamic DNS

Support Dynamic DNS-IP Binding

Provide DDNS analyze to help access dynamic data center

Flux Management

Support rate limiting,

Firewall Function

Package filtering

Port Mapping

Virtual Address Mapping

DMZ zone

MAC addresses binding.

Route function

Support Static Routing Table

VPN (not available for IR701/704)

IPSec VPN

L2TP VPN

GRE

Link Backup

VRRP

Support VRRP protocols, realizing immediate link backup

DNS Forwarding

Support DNS Forwarding, support DNS record

Network tools

Support Ping, Trace Route and Telnet

1.3.3 Environmental Limits

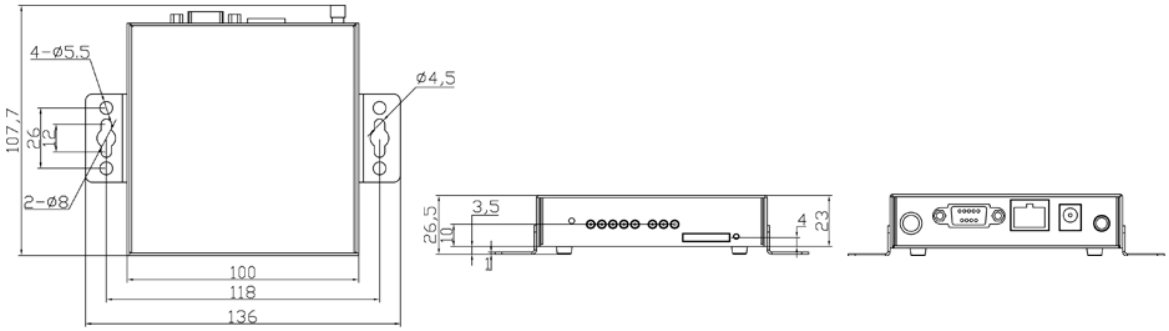
Operating Temperature: -20 to 70℃
Operating Humidity: 5 to 95% RH
Storage Temperature: -40 to 85℃

1.3.4 Power Requirements

Power Inputs: 1 terminal block, including power jack and serial.
Input Voltage: 5 -26 VDC

1.3.5 Physical Characteristics

Housing: Steel, providing IP30 protection
Weight: 490g
Dimensions (mm)



1.3.6 Advanced Industrial Characteristics

Physical Characteristics:
Shell: Metal, IP30

1.3.7 Device Management Software

Device Manager:
Centralized management solution for InHand Networks Devices

1.3.8 Warranty

Warranty Period: 1 year (Optional service for 3 years)

1.4 Product Models

The current models of InRouter 600 Series include: InRouter 601/611.

The models are classified according to main difference including cellular network, VPN support and interface for device.

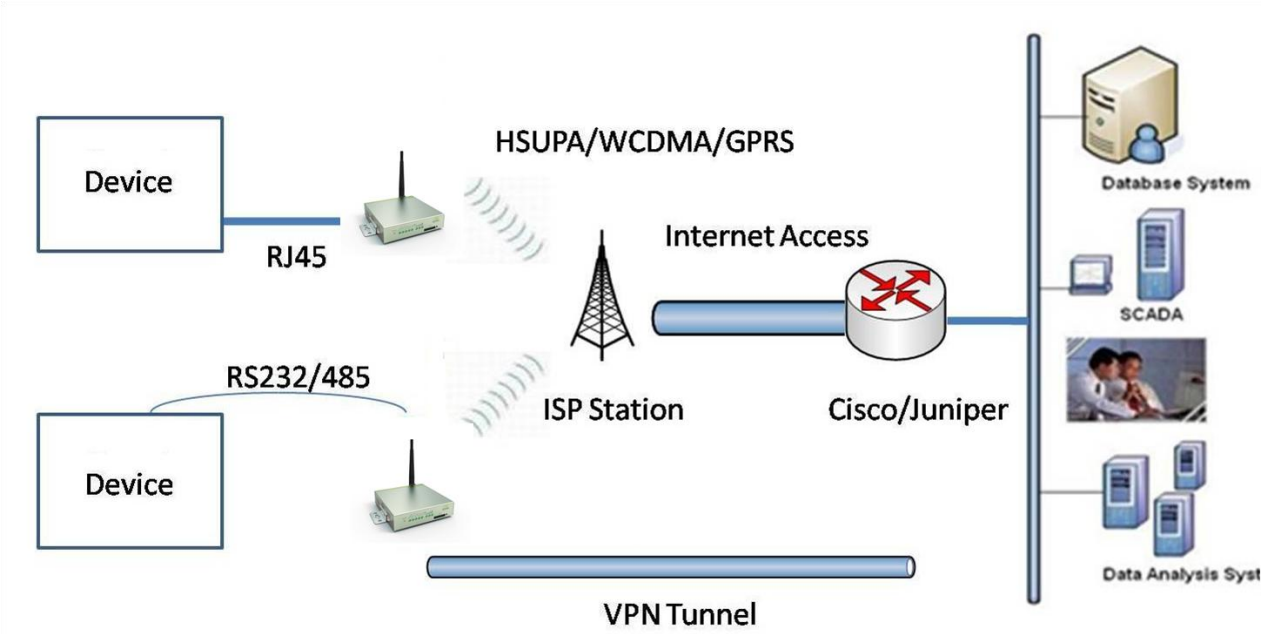
Model	Serial	LAN	Cellular WAN	Ethernet WAN	VPN
WCDMA					
IR601WH01-232	RS232	1 RJ45	HSUPA /HSDPA/WCDMA: 850/900/1900/2100MHz GSM/GPRS/EDGE: , 850/900/1800/1900MHz	N/A	FIREWALL
IR601WH01-485	RS485	1 RJ45	HSUPA /HSDPA/WCDMA: 850/900/1900/2100MHz GSM/GPRS/EDGE: , 850/900/1800/1900MHz	N/A	FIREWALL
IR611WH01-232	RS232	1 RJ45	HSUPA /HSDPA/WCDMA: 850/900/1900/2100MHz GSM/GPRS/EDGE: , 850/900/1800/1900MHz	N/A	FIREWALL&IPSec/L2TP/GRE
IR611WH01-485	RS485	1 RJ45	HSUPA /HSDPA/WCDMA: 850/900/1900/2100MHz GSM/GPRS/EDGE: , 850/900/1800/1900MHz	N/A	FIREWALL&IPSec/L2TP/GRE

II

Quick Installation Guide

- Typical Application
- Panel Layout
- Quick Connect to Internet
- Quick IPSec VPN Configuration
- Reset to Factory Defaults

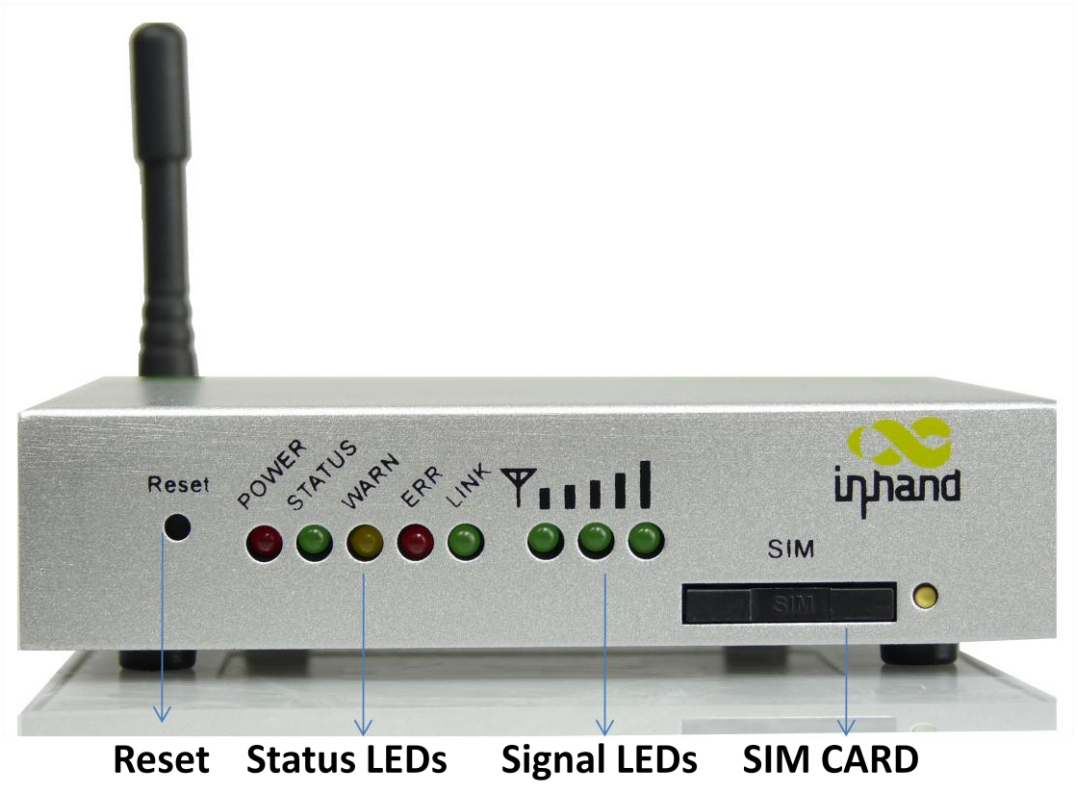
2.1 Typical Application



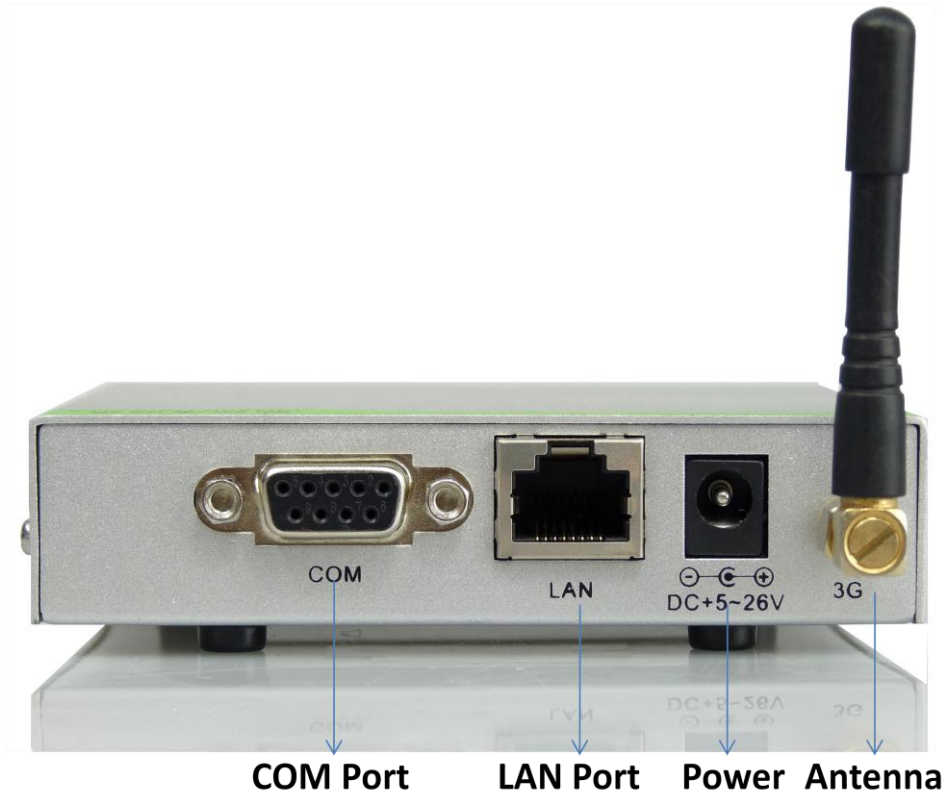
InRouter 600 series can be used to connect your device(with RS232/485/Ethernet Interface) to internet via GPRS/HSUPA cellular. Meanwhile, to ensure the security and access, InRouter 600 series support VPN, enabling remote access and secure data transmission through internet.

2.2 Panel Layout

Front:



Back:



Interface	Description
Power Interface	Access 5-26V DC Power Supply
Serial	Access to the serial line, realizing
Ethernet Ports	One 10/100Base-TX RJ45 Port (IR601,IR611)
ANTENNA	2.5G/3G antenna
SIM Card Connector	Put SIM card

Description of LED

Legend: On-- **Off--** **Blink--**

Power on

Start to run firmware

Begin dial to Internet

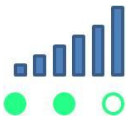
Connect to internet

Upgrading firmware

Restore factory default

Signal Status LED Description

----- Signal: 1-9 (bad signal level, route cannot work, please check the antenna and local signal level)



------ Signal: 10-19 (Router work normally under this signal level)

------ Signal: 20-31 (Perfect signal level)

2.3 Quick Connection to Internet

2.3.1 Insert SIM Card

Push the yellow button next to SIM, then insert SIM CARD.

2.3.2 Antenna Installation

After install the IR601, connect the interface of enhanced antenna and the interface of skin antenna and screw closely. Put the amplifier of enhanced antenna to where there receives good signal.

Attention: The position and angle may influence the quality of signal.

2.3.3 Power Supply

Link the power supply in the product package with InRouter, watch where the InRouter Power LED on the panel is light up. If not, please connect with InHand for technical supports.
You can configure IR600 after the Power LED lights up.

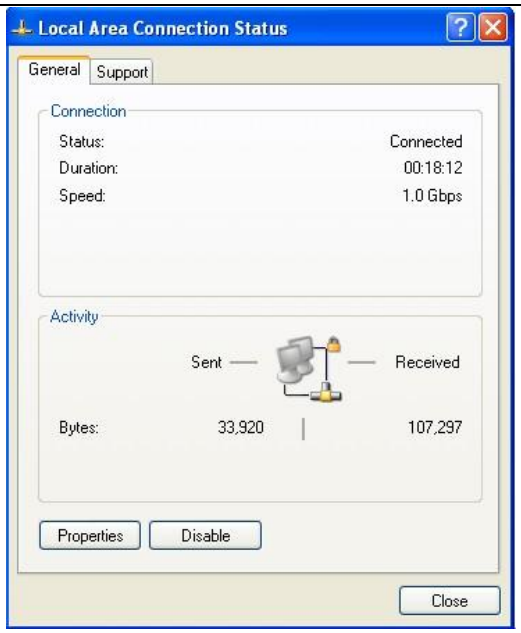
2.3.4 Connect

Link the IR600 with PC:
(1) Using the cable to link IR600 with PC;
(2) After the connection, you can see one LED of RJ45 Interface turns green and the other flashes.

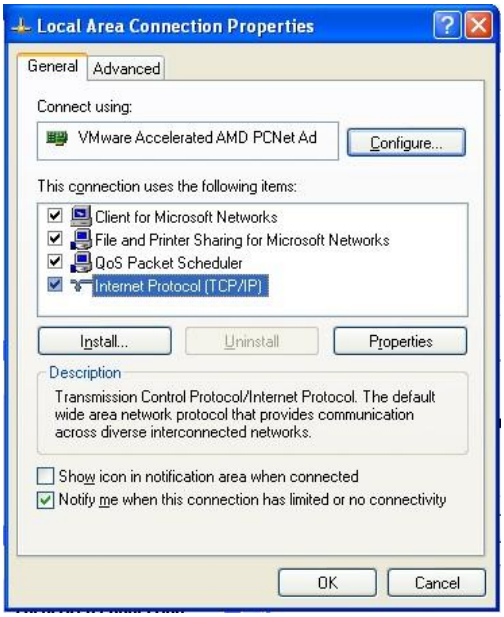
2.3.5 First Connect InRouter with Your PC

IR600 Router can auto-distribute IP address for PC. Please set the PC to automatically obtain IP address via DHCP. (Based on the Windows operation system):

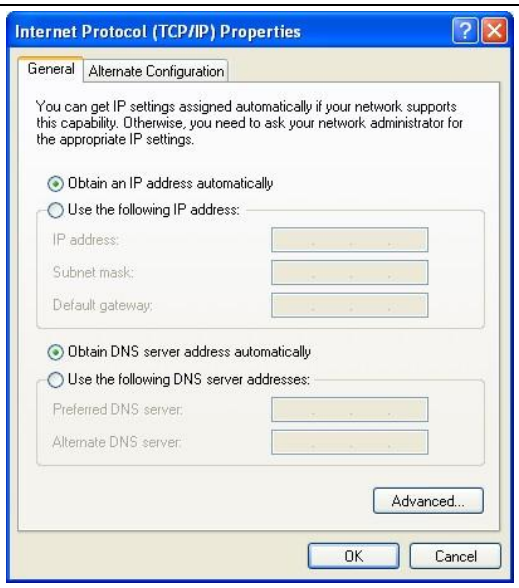
1) Open "Control Panel", double click "Network Connections" icon, and enter "Network Connections" Screen.
2) Double click "Local Area Connection", enter "Local Area Connection Status" screen:



3) Click "Properties", enter "Local Area Connection Properties" screen



Choose "Internet Protocol (TCP/IP)", click "properties" button, ensure your PC can obtain IP and DNS address automatically. (Or you can set your PC in the subnet: 192.168.2.0/24, for example, set IP: 192.168.2.10, Net Mask: 255.255.255.0, Default Gateway: 192.168.2.1)

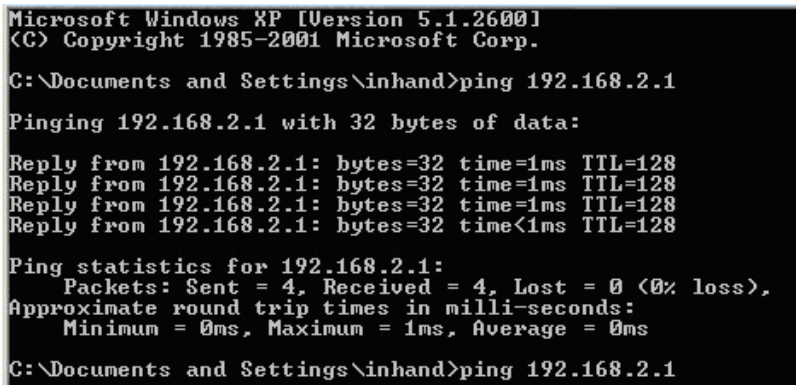

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Click "OK", InRouter will allocate an IP address: 192.168.2.X, and a gateway: 192.168.2.1(the default address of IR600).

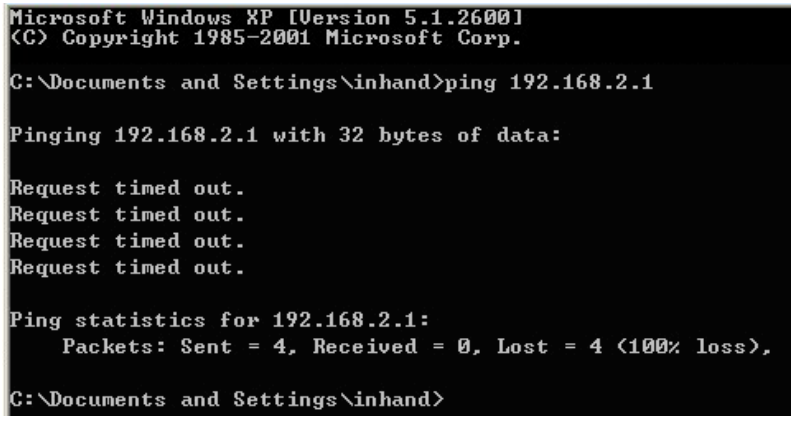
After configure TCP/IP protocols, you can use ping command to check whether the link between PC and Router is built correctly. There is an example to execute Ping command under Windows XP as below:

Ping 192.168.2.1

If the screen shows:


Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\inhand>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Documents and Settings\inhand>ping 192.168.2.1

Then the link between the PC and Router is correct connected. Else if it shows:

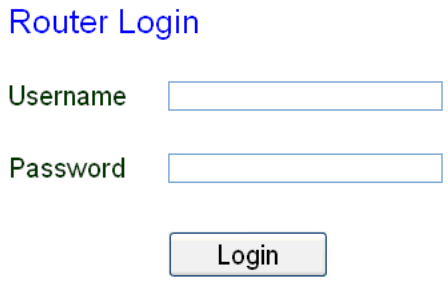

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\inhand>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Documents and Settings\inhand>

Then the connection seems not build, and you need to check thoroughly following the former instructions.

2.3.6 Start to configure your InRouter 600(Optional)

After you have finished the former steps, you can configure the Router:

1) Open IE browser, input the default IP address of the Router: http://192.168.2.1, you can see the login web below:

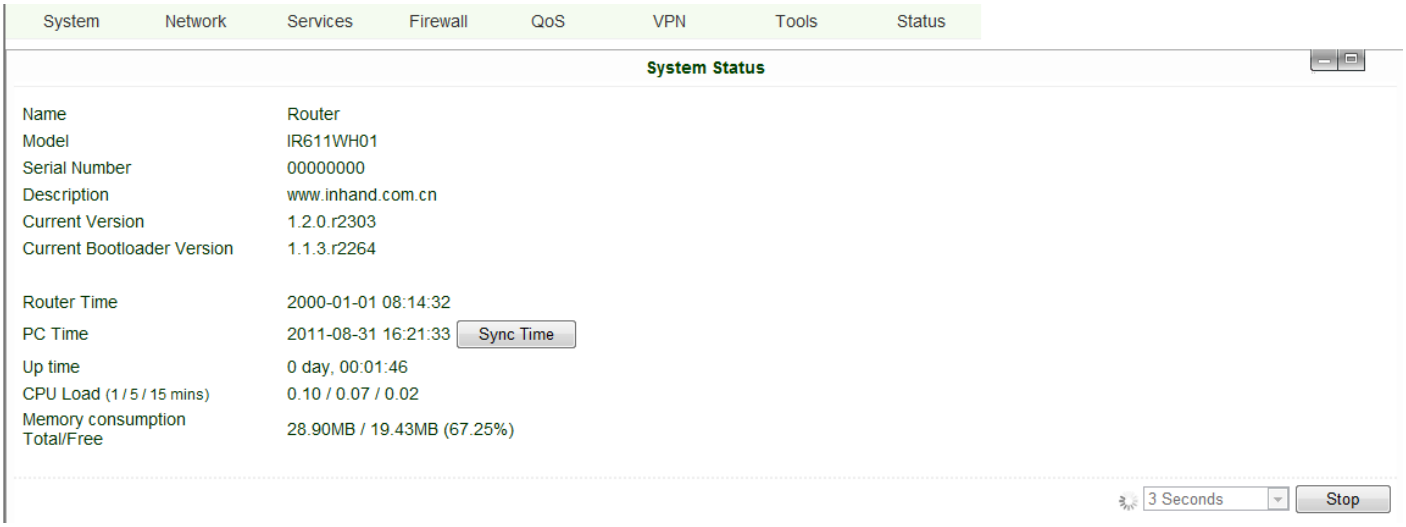


Input "username" (default: adm) and the "password" (default: 123456), and then click "login" to enter the operation screen.

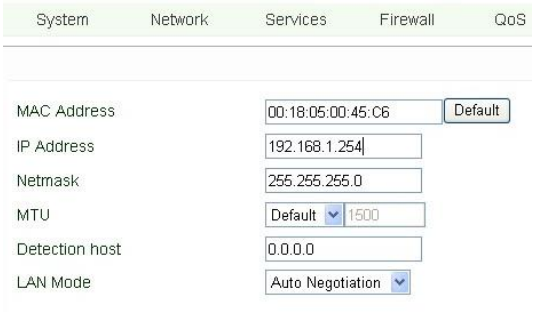
2) Change the IP configuration:

Attention: After configuration, please click "apply" to activate your configuration.

If you want to set your own IP of InRouter 600, please follow the instructions below:


System Network Services Firewall QoS VPN Tools Status
System Status
Name Router
Model IR611WH01
Serial Number 00000000
Description www.inhand.com.cn
Current Version 1.2.0.r2303
Current Bootloader Version 1.1.3.r2264
Router Time 2000-01-01 08:14:32
PC Time 2011-08-31 16:21:33 Sync Time
Up time 0 day, 00:01:46
CPU Load (1 / 5 / 15 mins) 0.10 / 0.07 / 0.02
Memory consumption Total/Free 28.90MB / 19.43MB (67.25%)
3 Seconds
Stop

Click "Network"=>"LAN", change the IP address to 192.168.1.254:



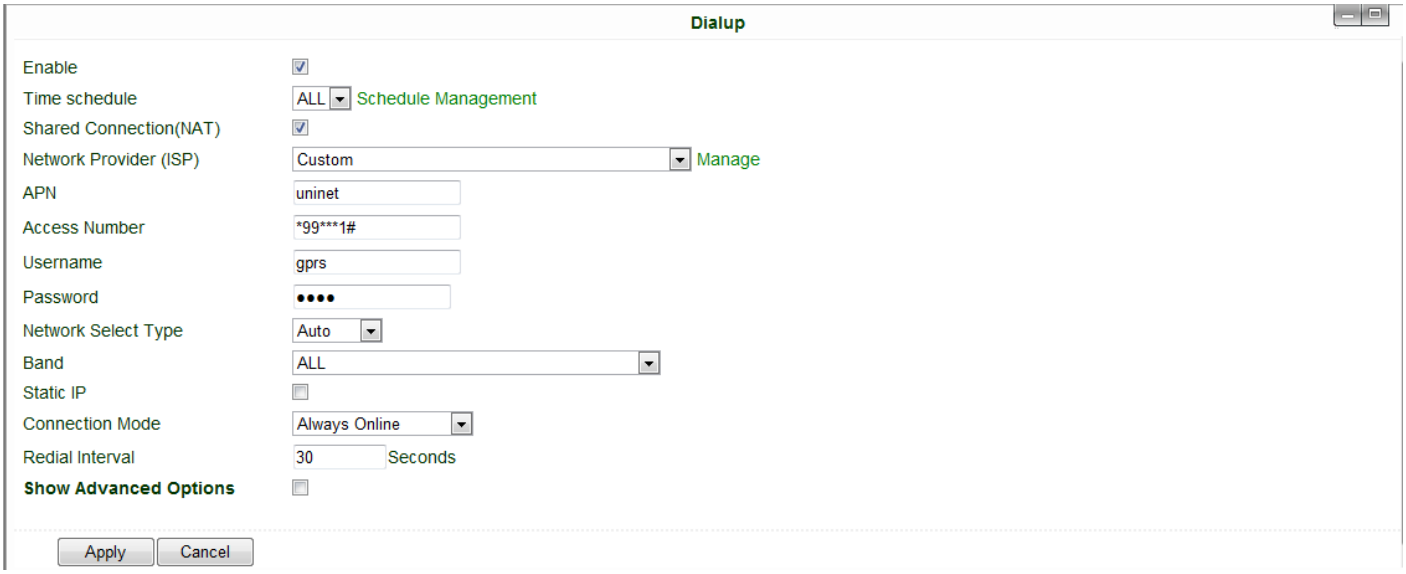
3) Click "Apply", then you will see:

Now the IP address of IR600 has been reset, and in order to enter the configuration web, you need set your PC in the same subnet, for example: 192.168.1.10/24 then input the changed IP address (192.168.1.254) in your IE Browser.

2.3.7 Connect InRouter with Internet

Following the configuration steps below to enable IR600 to connect with the internet.

Click "Network"=>"Dialup", enter dialup configuration web:



Please check the APN, Dialup Number, Username and Password:

Dialup Number, Username and Password are provided by local mobile operator. You can contact them for more details.

The following example shows parameters provided by China Mobile, Vodafone and Cingular. Please contact with local operator for details.

1: China Mobile

APN: CMNET

Phone Number: *99#

User Name: web

Password: web

2: Vodafone

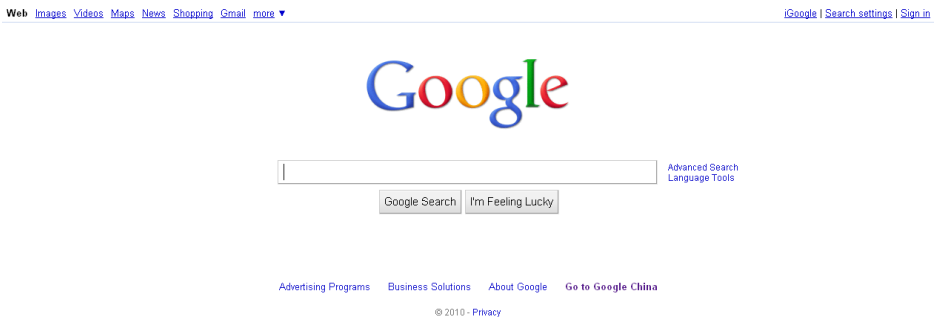
APN: internet

Phone Number: *99#

User Name: web

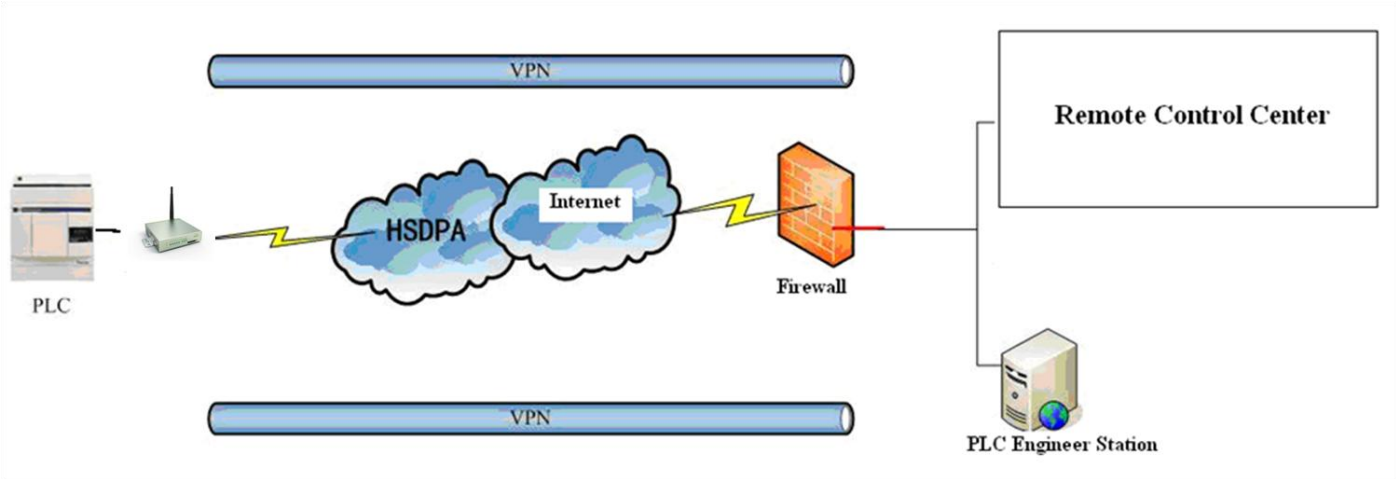
Password: web

After correct configuration, InRouter 600 can now connect with Internet. Open IE Browser, input www.google.com, you can see the Google web as below:

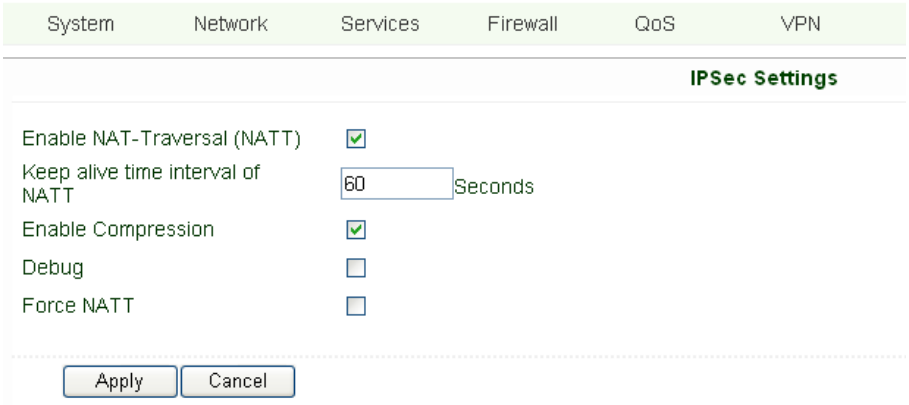


2.4 Quick IPSec VPN Configuration

If you need to build a VPN tunnel to realize access to your PLC far away through internet or you need ensure the security by using VPN. Here's a quick configuration guide of IPSec for InRouter 600 Series.



Connect PC with Router to enter router configuration web, select "VPN" => "IPSec setting":



Enable NAT-Traversal (NATT): select enable.

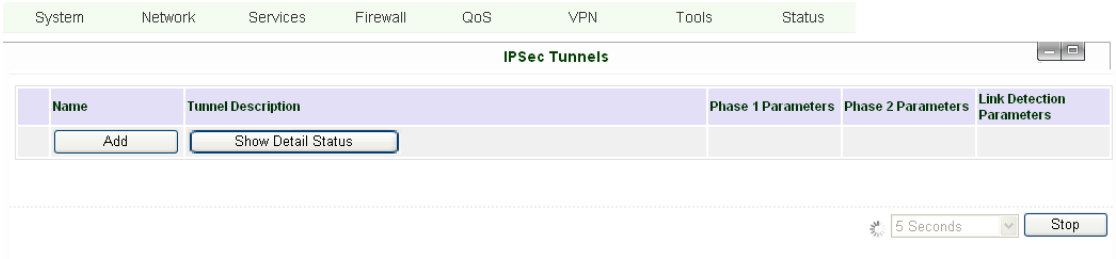
Keep alive time interval of NATT: set the "Keep alive time interval of NATT", default is 60 seconds.

Enable Compression: select enable.

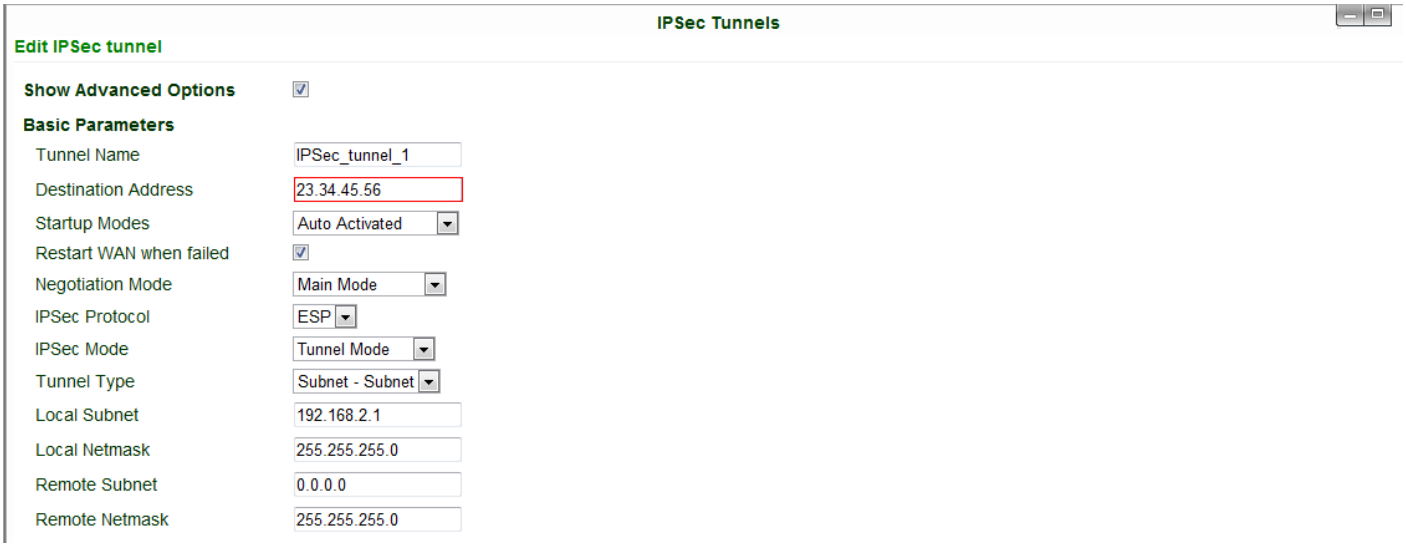
Please change the parameters according to concrete situation.

Click "Apply" to finish configuration.

1） Select "VPN"=> "IPSec Tunnels" to check or modify parameters of IPSec Tunnels.



Click "Add" to add a new IPSec Tunnel:



Basic Parameters: set basic parameters of IPSec tunnel.

Tunnel Name: name IPSec tunnel, the default is IPSec_tunnel_1.

Destination Address: set to VPN server IP/domain, e.g.: the domain provided by GJJ is gjj-ovdp.3322.org.

Startup Modes: select Auto Activated.

Negotiation Mode: optional between Main Mode and Aggressive Mode. Generally, select Main Mode.

IPSec Protocols: optional among ESP, AH. Generally, select ESP.

IPSec Mode: optional between Tunnel Mode and Transport Mode. Generally, select Tunnel Mode.

Tunnel Type: optional among Host-Host, Host-Subnet, Subnet-Host and Subnet-Subnet.

Local Subnet: IPSec local subnet protected. E.g.: 172.16.16.0.

Local Net Mask: IPSec local Net Mask protected. E.g.: 255.255.255.252.

Remote Subnet: IPSec remote subnet protected. E.g.: 172.16.0.0.

Remote Net Mask: IPSec remote Net Mask protected. E.g.: 255.240.0.0.

Phase 1 Parameters: configure parameters during the Phase 1 of IPSec negotiation.

IKE Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IKE Lifetime: the default is 86400 seconds.

Local ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Remote ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Authentication Type: optional between Shared Key and Certificate, generally choose Shared Key.

Key: set IPSec VPN negotiating key.

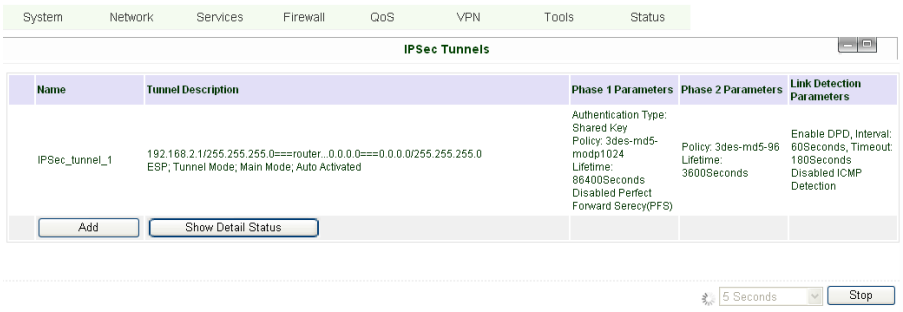
Phase 2 Parameters: configure parameters during the Phase 2 of IPSec negotiation.

IPSec Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IPSec Lifetime: the default is 3600 seconds.

Perfect Forward Encryption: Optional among None, GROUP1, GROUP2 and GROUP5. This parameter should match with the server, generally, select "None".

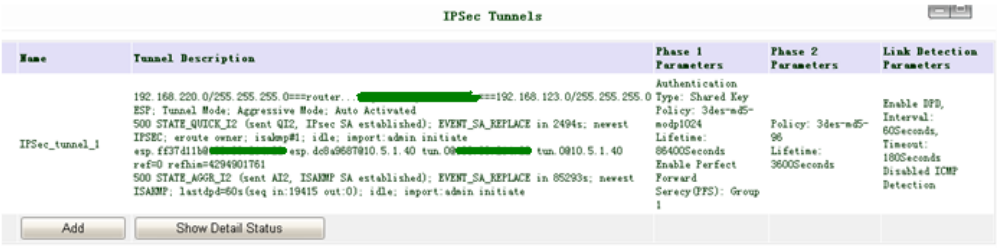
Click "Save" to finish adding IPSec Tunnel:



You can click "Show Detail Status" to observe the specific connection details, or click "Add" to add a new tunnel.

Now you succeed to build a high-security IPSec tunnel, here's an example:

We set an IPSec Tunnel from subnet: 192.168.220.0/24 to subnet: 192.168.123.0/24, when it succeeds, the web will show:


IPSec Tunnels
Name
Tunnel Description
Phase 1 Parameters
Phase 2 Parameters
Link Detection Parameters
IPSec_tunnel_1
192.168.220.0/255.255.255.0===router...===192.168.123.0/255.255.255.0
ESP; Tunnel Mode; Aggressive Mode; Auto Activated
500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2494s; newest IPSEC; eroute owner; isakmp#1; idle; import:admin initiate
esp.ff37d11b0 esp.dc8a868f@10.5.1.40 tun.0@ tun.0@10.5.1.40
ref=0 refhim=4294901761
500 STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 85293s; newest ISAKMP; lastdpd=60s(seq in:19415 out:0); idle; import:admin initiate
Authentication Type: Shared Key
Policy: 3des-md5-modp1024
Lifetime: 86400Seconds
Enable Perfect Forward Serecy(PFS): Group 1
Policy: 3des-md5-96
Lifetime: 3600Seconds
Enable DPD, Interval: 60Seconds, Timeout: 180Seconds
Disabled ICMP Detection
Add
Show Detail Status

And the PC in IPSec client subnet can get access to the server's subnet.

Open command in your PC, then ping a PC in the server's subnet:

```
C:\Documents and Settings\Jason Hu>ping 192.168.123.250

Pinging 192.168.123.250 with 32 bytes of data:

Reply from 192.168.123.250: bytes=32 time=428ms TTL=63
Reply from 192.168.123.250: bytes=32 time=395ms TTL=63
Reply from 192.168.123.250: bytes=32 time=397ms TTL=63
Reply from 192.168.123.250: bytes=32 time=393ms TTL=63
```

III

Advanced Configuration

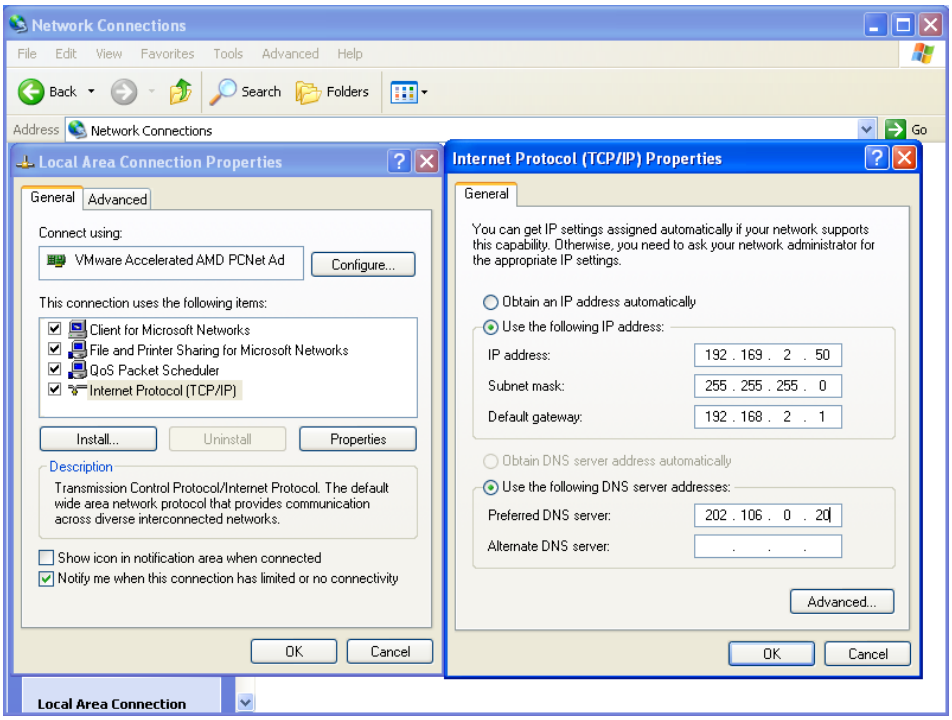
- Configuration on Web

3.1 Configuration on Web

InRouter must be correctly configured before use. This Chapter will show you how to configure via Web.

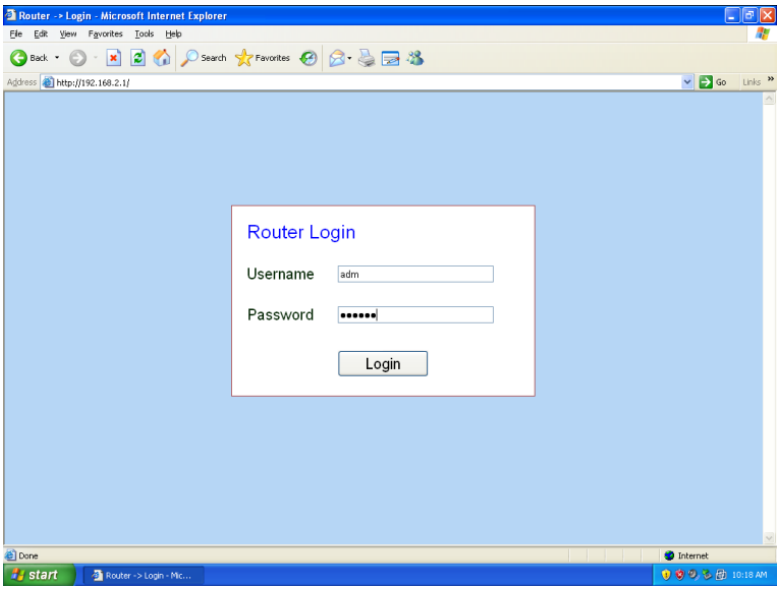
3.1.1 Preparation

Firstly, connect your devices with IR600 by cable or HUB (switch), then set the IP of PC and IR600 in the same subnet, for example: Set PC IP to 192.168.2.50, net mask: 255.255.255.0, gateway (default IP of IR600: 192.168.2.1):

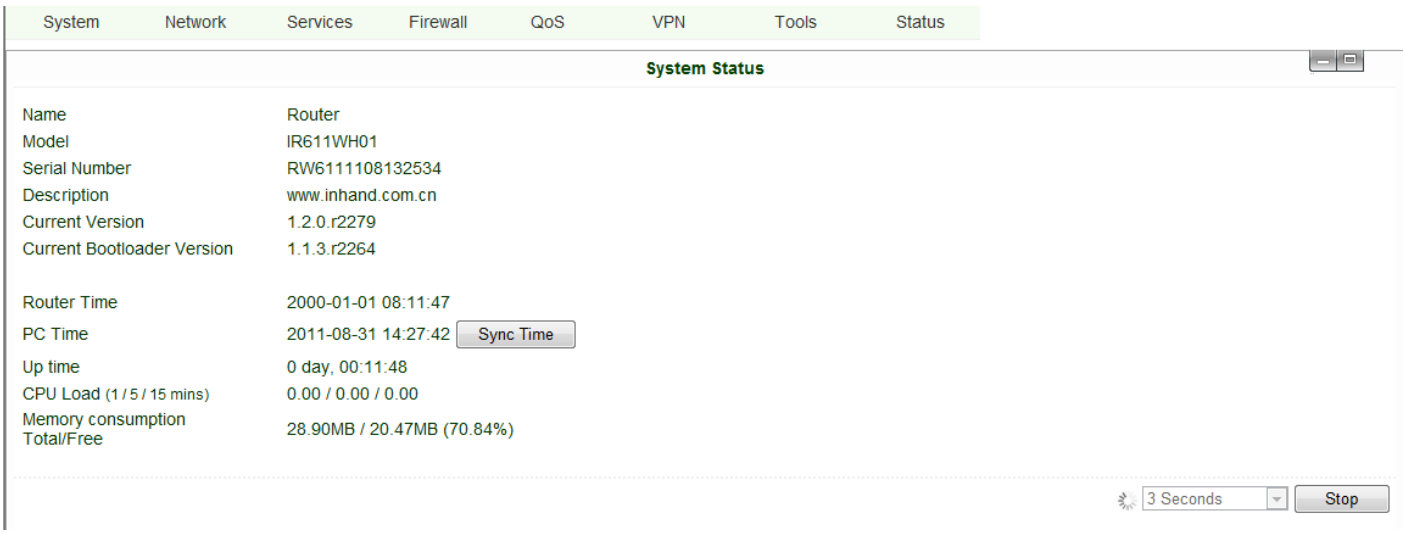

Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Local Area Connection Properties
General Advanced
Connect using:
VMware Accelerated AMD PCNet Ad
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK Cancel
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 169 . 2 . 50
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 2 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 202 . 106 . 0 . 20
Alternate DNS server:
Advanced...
OK Cancel
Local Area Connection

Open IE browser, input the IP address of IR600: http://192.168.2.1 (default IP of IR600).

Then you'll see the Login Web below, you need to login as Administrator. Input the username and password (default: adm/123456).



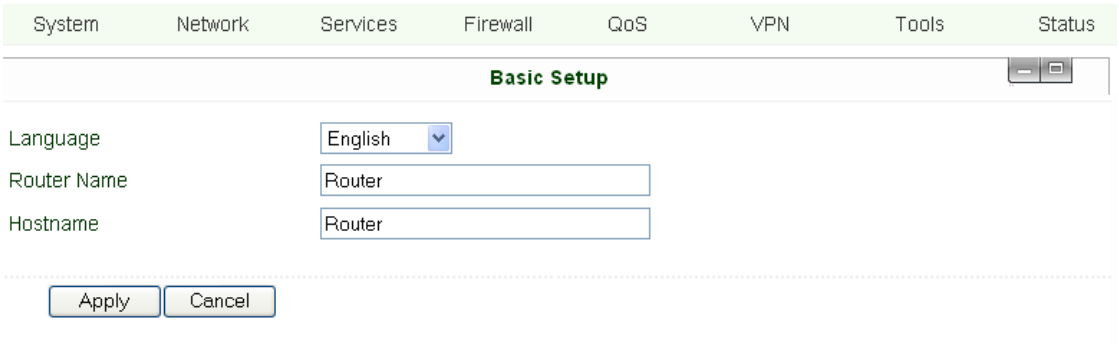
Click "Login" to enter configure web:



3.1.2 System

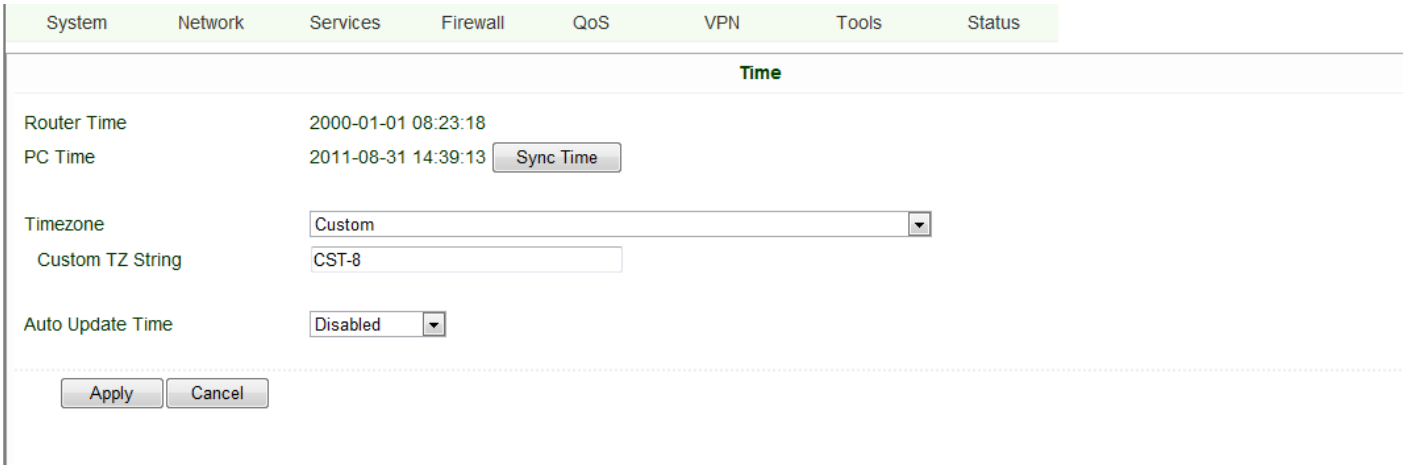
System settings include the 9 settings: Basic Setup, Time, Serial Port, Admin Access, System Log, Config Management, Update, Reboot and Logout.

(1) Basic Setup



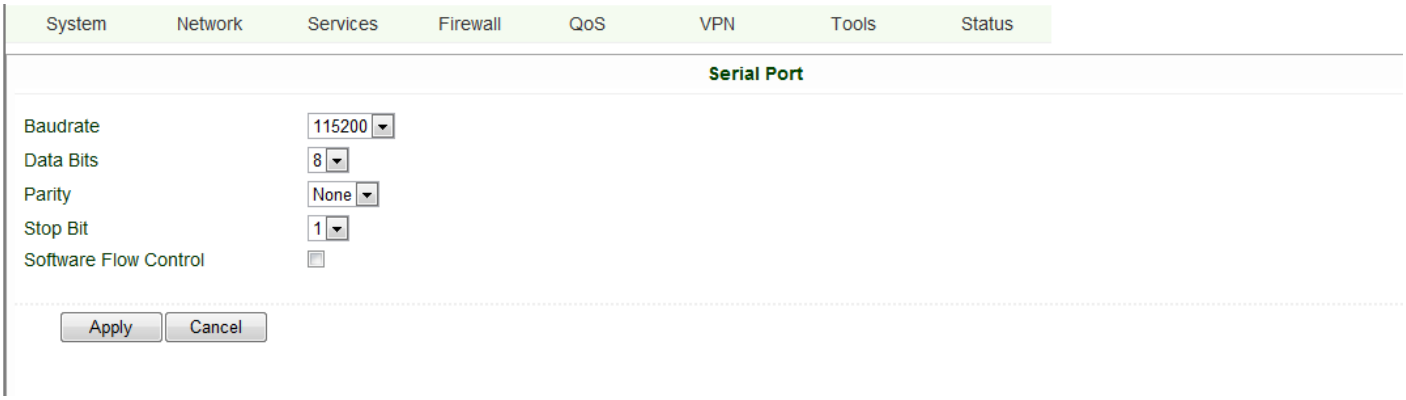
Parameters Name	Description	Default	Example
Language	Choose language of configuration web	Chinese	English
Router Name	Set name of InRouter	Router	My InRouter
Host Name	Name the device/PC linked with IR600	Router	My InRouter

(2) Time



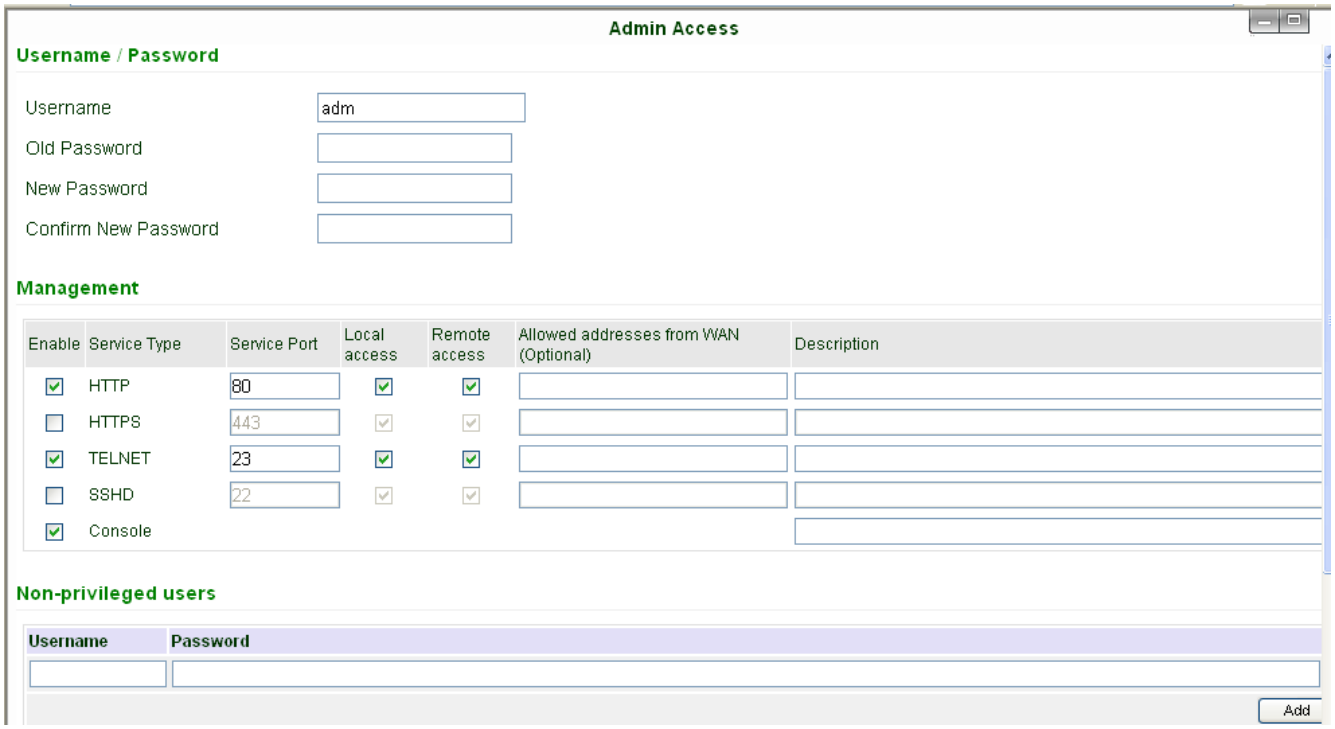
Name	Description	Default
Router Time	Display router time	2000-01-01 8:00:00
PC Time	Display PC time (or the time of device linked with router)	
Time Zone	Set time zone	Custom
Custom TZ string	Set the string of time zone of Router	CST-8
Auto Update Time	Time Update Interval	Disabled
NTP Time Servers (after enable the Auto Update Time)	Setting for NTP Time server. (Three at the most)	pool.ntp.org

(3) Serial Port



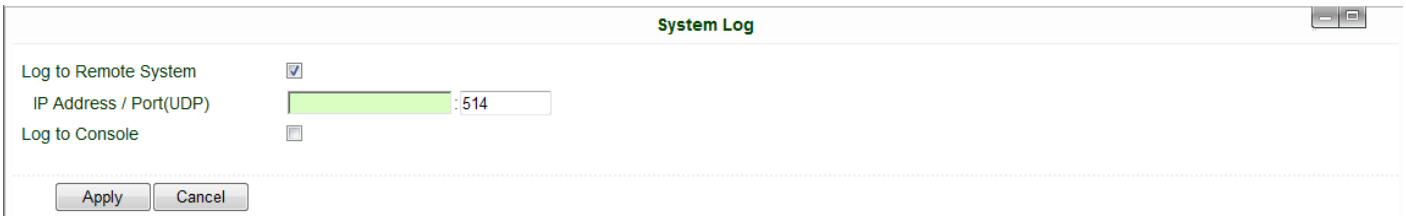
Name	Description	Default
Baud Rate	Serial baud rate	115200
Data Bit	Serial data bits	8
Parity	Set parity bit of serial data.	None
Stop Bit	Set stop bit of serial data.	1
Hardware Flow Control	Enable Hardware Flow Control	Disable
Software Flow Control	Enable Software Flow Control	Disable

(4) Admin Access



Name	Description	Default
Username/Password		
Username	Username for configuration web login	adm
Old Password	To change the password, you need to input the old one	123456
New Password	Input new password	
Confirm New Password	Input the new password again	
Management		
HTTP/HTTPS/TELNET/SSHD/Console		
Enable	Select to enable	Enable
Service Type	HTTP/HTTPS/TELNET/SSHD/Console	80/443/23/22/Blank
Local Access	Enable—allow manage Router by LAN(e.g.: HTTP) Disable—forbid manage Router by LAN.	Enable
Remote Access	Enable—allow to manage IR600 by WAN. (e.g.: HTTP) Disable—forbid to manage IR600 by WAN. (e.g.: HTTP)	Enable
Allowed Access from WAN (Optional)	Set the range of allowed IP address for WAN (HTTP/HTTPS/TELNET/SSHD)	Control services server can be set at this time, for example 192.168.2.1/30 or 192.168.2.1-192.168.2.10
Description	Describe the parameters of management (non-influence to IR600)	
Other Parameters		
Log Timeout	Set the Log Timeout, configuration web will be disconnected after timeout	500 seconds

(5) System Log

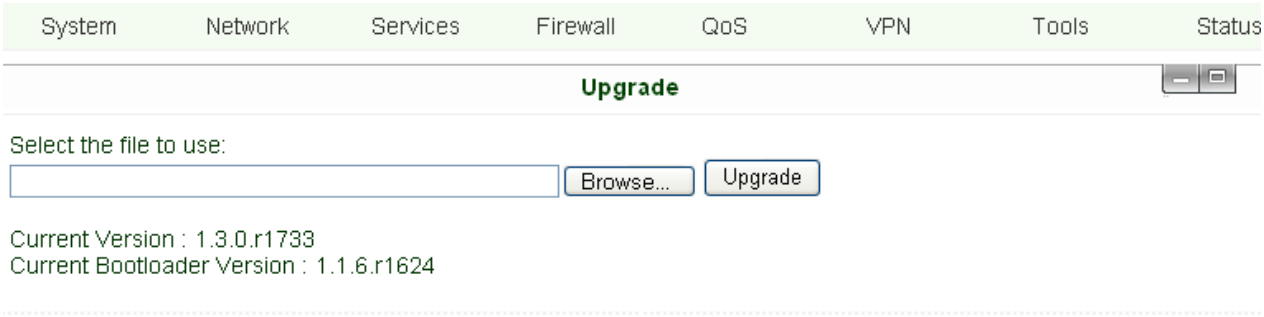


Name	Description	Default
Log to Remote System	Enable remote log server	Disable
IP address/Port (UDP)	Set the IP and Port of remote log server	Port: 514
Log to Console	Enable remote log server	Disable

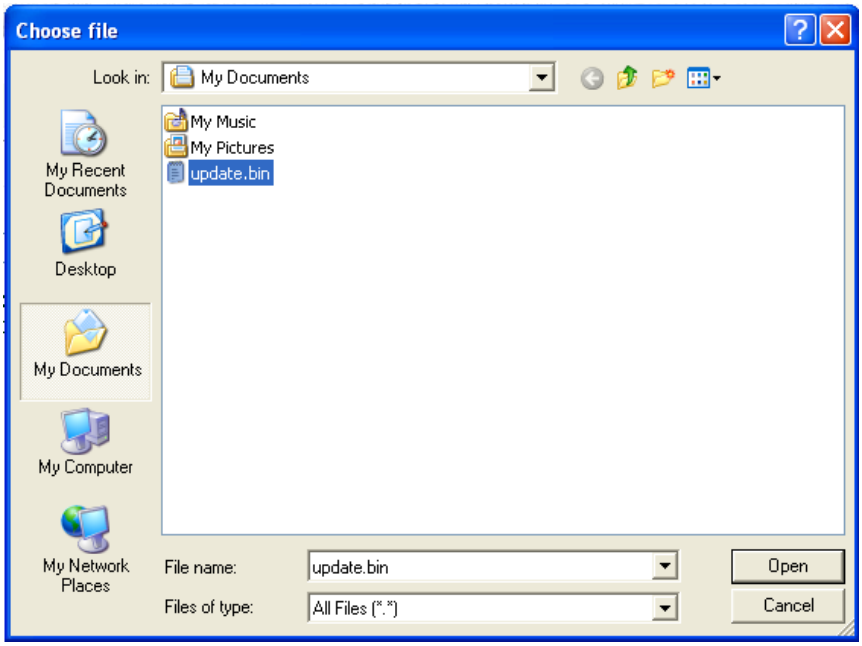
(6) Config Management

Name	Description
Router Configuration	Import/Backup configuration file
Restore default configuration	Click to reset IR600 (to enable RESET, you need to reboot IR600)
Network Provider (ISP)	Used to configure the APN, username, password and other parameters of major operators

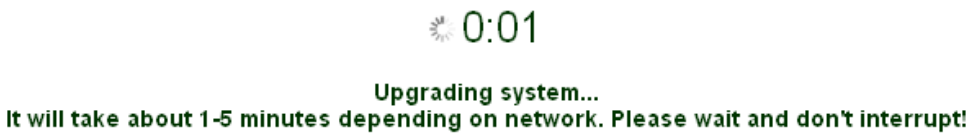
(7) System Upgrade



If need to upgrade system, click "System"=>"System upgrade" to enter update page, then follow the steps below:
Click "Browse", choose the upgrade file;



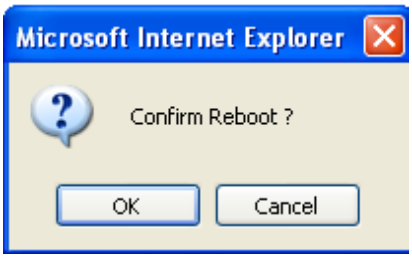
Click "update", and then click "sure" to begin update as it shows below.



Upgrade firmware succeed, and click "reboot" to restart IR600.

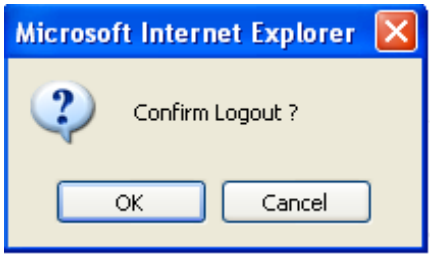
(8) Reboot

If you need to reboot system, please click "System"=>"Reboot", Then click "OK" to restart system.



(9) Logout

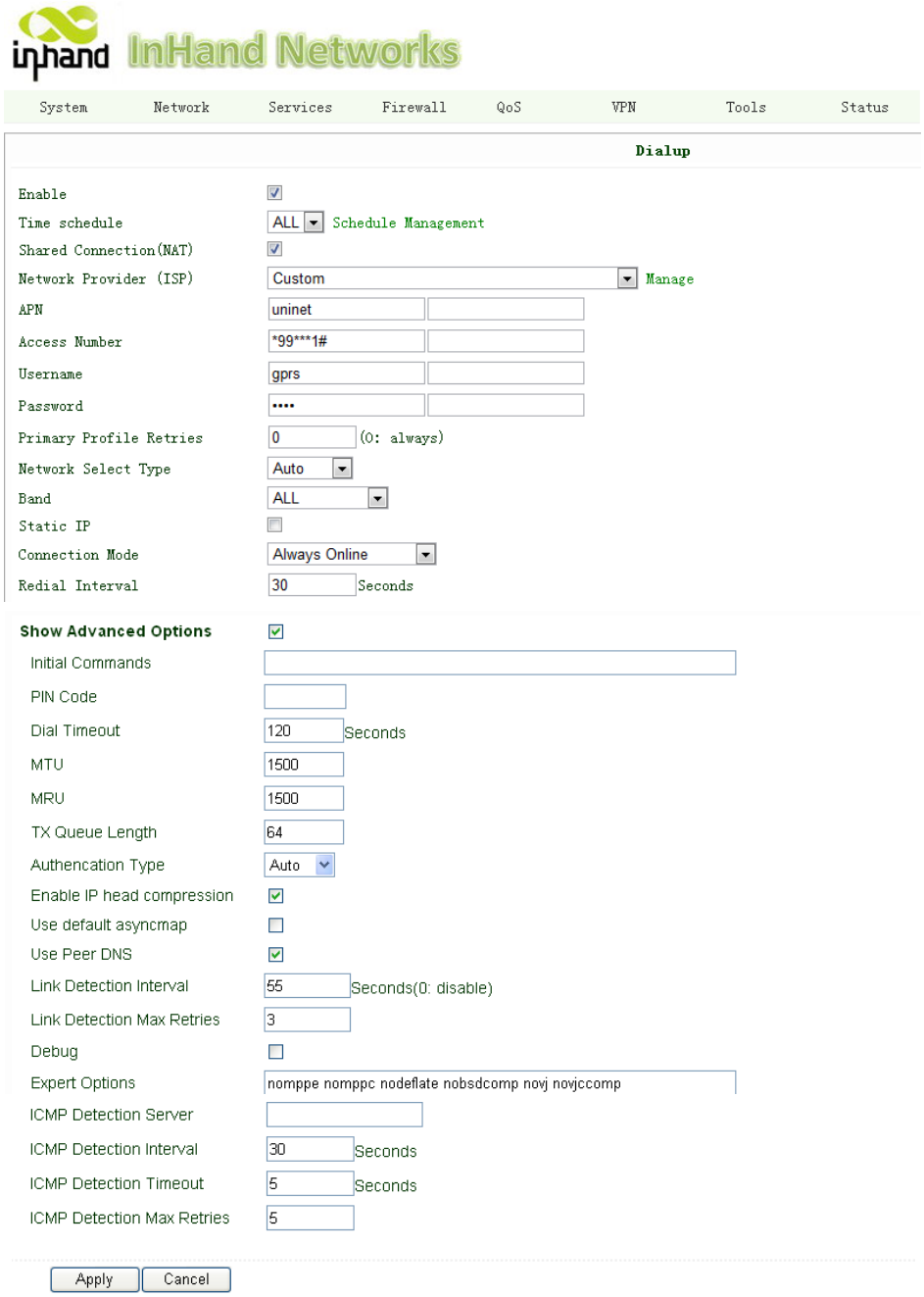
If you need to logout system, click "System"=>"Logout", and then click "OK".



3.1.3 Network

Network settings include configurations of Dialup, LAN, DNS, DDNS, Static Route, and etc.

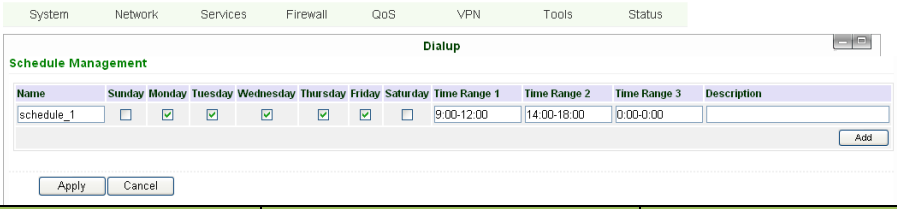
(1) Dialup



Name	Description	Default
Enable	Enable PPP dialup	Enable
Time Schedule	Set time for online and offline	ALL
SHARED	Enabled—device linked with Router **Can** access to internet. Disable—device **Can NOT** access to internet via Router.	Enable
ISP	Select local ISP, if not listed here, please select "Customer"	Customer
Network Select Type	Choose mobile network type	HSDPA (or GPRS)

APN	APN parameters provided by **Local ISP, you can set TWO different group of dialup parameters (APN/Username/Password) and set one as backup**	cmnet/uninet
Access Number	Dialup parameters provided by **Local ISP**	"*99#""*99***1#" or #777
Username	Dialup parameters provided by **Local ISP**	"gprs" or "CDMA"
Password	Dialup parameters provided by **Local ISP**	"gprs" or "CDMA"
Primary Profile Retries	After retries and dialup still failed, router will try backup dialup parameters (if you have set two IPSec tunnels and one as backup, router will also stop the main one and try another, more details please see at "VPN" → "IPSec")	0 (always use main parameters and never use backup)
Static IP	Enable Static IP if your SIM card can get static IP address	Disable
Connection Mode	Optional Always Online,	Always Online
Redial Interval	When Dial fails, InRouter will redial after the interval	30 seconds
Show Advanced Options	Enable configure advanced options	Disabled
Initial Commands	Used for advanced parameters	Blank
Dial Timeout	Set dial timeout (IR600 will reboot after timeout)	120 seconds
MTU	Set max transmit unit	1500
MRU	Set max receive unit	1500
TX Queue Length	Set length of transmit queue	3
Enable IP header compression	Enable IP header compression	Disabled
Use default asyncmap	Enable default asyncmap, PPP advanced option	Disabled
Using Peer DNS	Click Enable to accept the peer DNS	Enabled
Link Detection Interval	Set Link Detection Interval	30 seconds
Link Detection Max Retries	Set the max retries if link detection failed	3
Debug	Enable debug mode	Enable
Expert Option	Provide extra PPP parameters, normally user needn't set this.	Blank
ICMP Detection Server	Set ICMP Detection Server, blank represents none	Blank
ICMP Detection Interval	Set ICMP Detection Interval	30 seconds
ICMP Detection Timeout	Set ICMP Detection Timeout (IR600 will reboot if ICMP time out)	5 seconds
ICMP Detection Max Retries	Set the max number of retries if ICMP failed	5

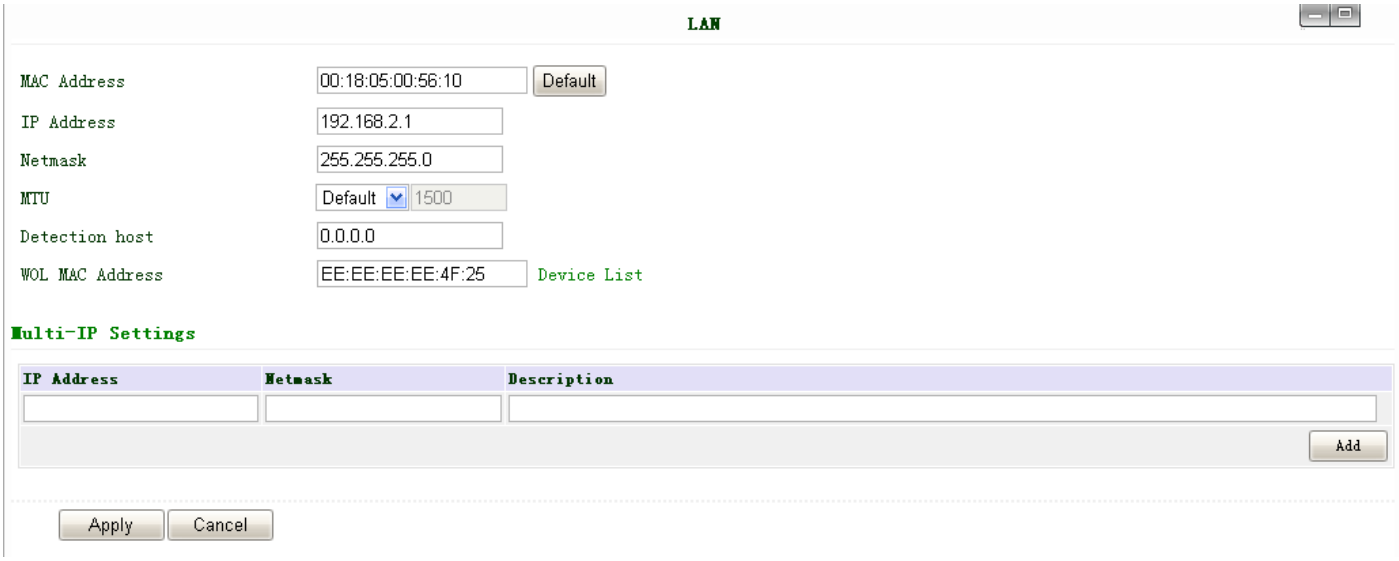
Dialup----Time Schedule Management:



Name	Description	Default
Name	Name the schedule	schedule 1
Sunday		Blank
Monday		Enable
Tuesday		Enable
Wednesday		Enable
Thursday		Enable
Friday		Enable
Saturday		Blank
Time Range 1	Set Time Range 1	9:00-12:00

Time Range 2	Set Time Range 2	14:00-18:00
Time Range 3	Set Time Range 3	0:00-0:00
Description	Describe configuration	Blank

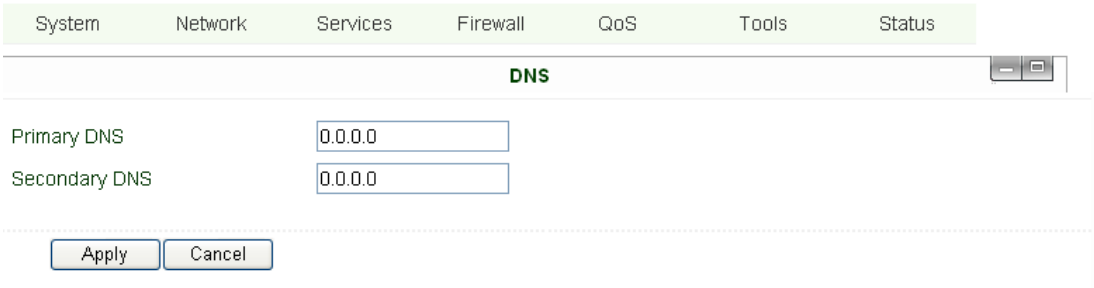
(2) LAN



Notice: please **DO NOT** set LAN address as: 192.168.3.x (an IP for DMZ port).

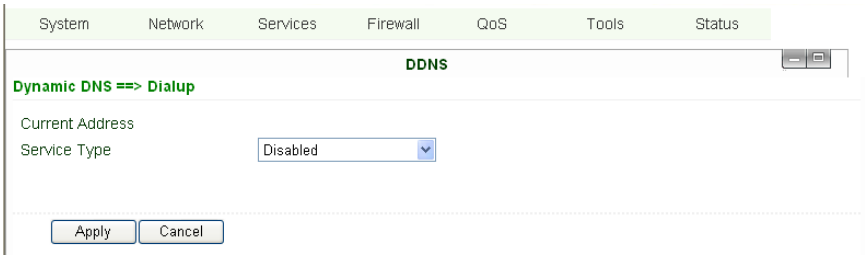
Name	Description	Default
MAC Address	The MAC address in LAN	00:10:A1:86:95:02 (Provided by InHand) , for manufactures
IP Address	Set IP Address in LAN	192.168.2.1 (If Changed, you need to input the new address for entering the configuration web)
Net Mask	Set Net Mask of LAN	255.255.255.0
MTU	Set MTU length, optional between Default and Manual	1500
Detection Host	Set Detection Host Address	0.0.0.0
WOL MAC Address	Set the MAC of PC in the LAN of router, for Wakeup Over LAN (WOL) function, you should also set "Networks"→ "Dialup" and change dialup mode into "Trigger by SMS".	Blank
Multi-IP Settings (Support additional 8 IP addresses at the most)		
IP Address	Set additional IP Address of LAN	Blank
Description	Description about this IP address	Blank

(3) DNS

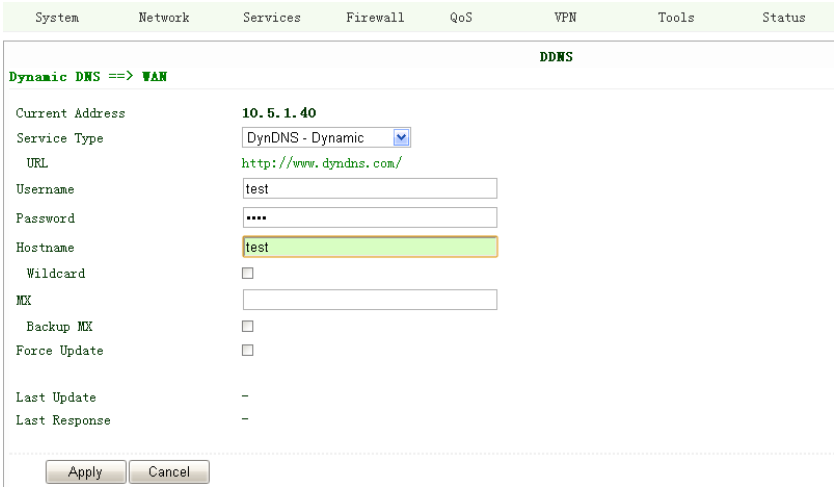


Name	Description	Default
Primary DNS	Set Primary DNS	Blank
Secondary DNS	Set Secondary DNS	Blank

(4) DDNS (Dynamic DNS)

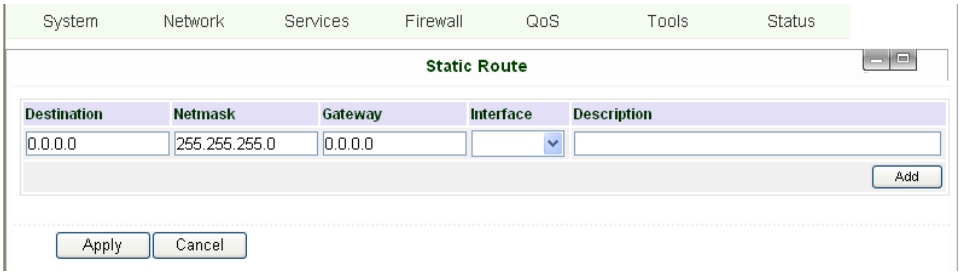


Name	Description	Default
Current Address	Show the current IP address	Blank
Service Type	Select DDNS Provider	Disabled



Name	Description	Default
Service Type	DynDNS - Dynamic	
URL	http://www.dyndns.com/	
Username	Registered username for DDNS	
Password	Registered password for DDNS	
Hostname	Registered hostname for DDNS	

(5) Static Route



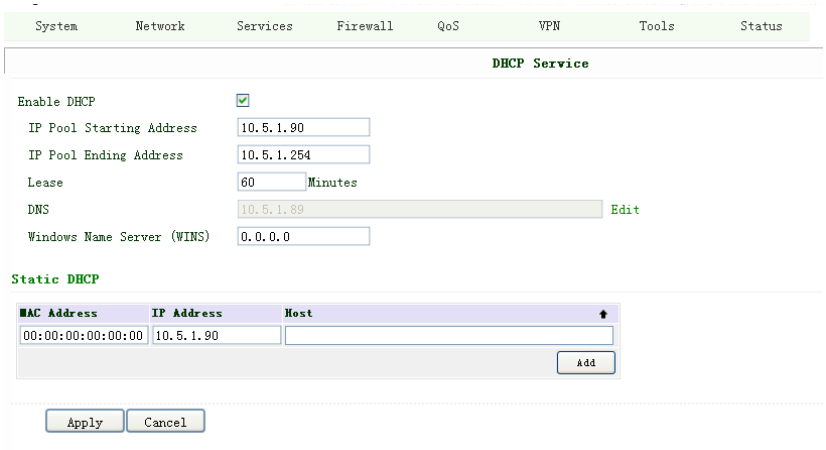
Name	Description	Default

Destination	Set IP address of destination	Blank
Net Mask	Set subnet Mask of destination	255.255.255.0
Gateway	Set the gateway of destination	Blank
Interface	Optional LAN/WAN port access to destination	Blank
Description	Describe static route	Blank

3.1.4 Service

Service settings include DHCP Service, DNS Forwarding, VRRP and other related parameters.

(1) DHCP Service

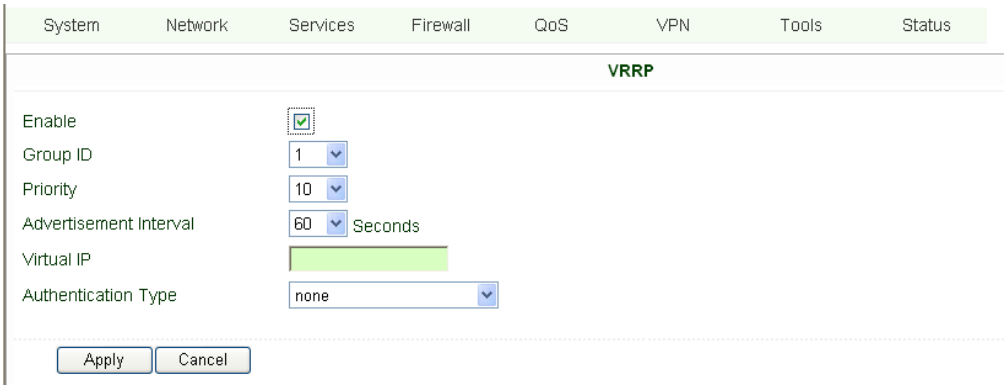


Name	Description	Default
Enable DHCP	Click to enable DHCP	Enable
IP Pool Starting Address	Set the starting IP address of DHCP pool	192.168.2.2
IP Pool Ending Address	Set the ending IP address of DHCP pool	192.168.2.100
Lease	Set the valid time lease of IP address obtained by DHCP	60 minutes
DNS	Set DNS Server	192.168.2.1
Windows Name Server (WINS)	Set WINS	Blank
Static DHCP (can set 20 designated IP address at the most)		
MAC Address	Set the MAC address of a designated IP address	Blank
IP address	Set the static IP address	192.168.2.2
Host	Set the hostname	Blank

(2) DNS Relay

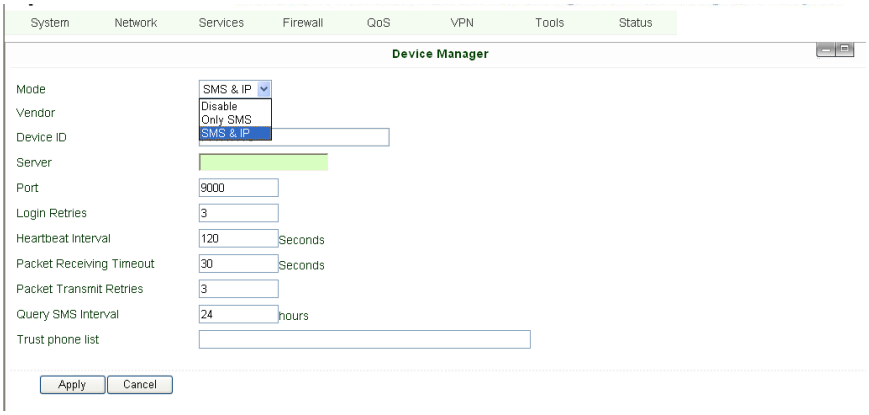
Name	Description	Default
Enable DNS Relay	Click to enable DNS Relay	Disabled
Designate IP address<=>DNS couples (20 at the most)		
IP Address	Set IP address <=> DNS couples	Blank
Host	Set the name of IP address <=> DNS couples	Blank
Description	Describe IP address <=> DNS couples	Blank

(3) VRRP

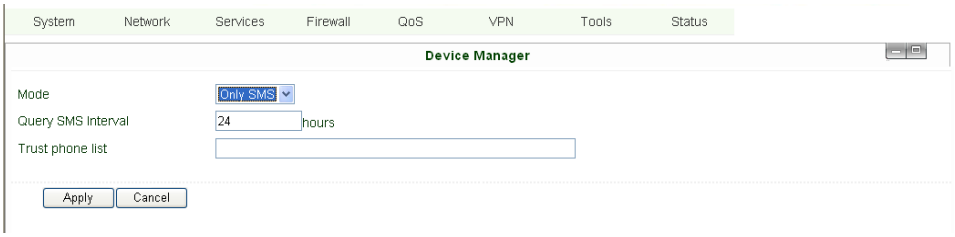


Name	Description	Default
Enable	Select to enable VRRP	Disable
Group ID	Select group id of routers (range 1-255)	1
Priority	Select priority for router (range 1—254)	10 (bigger number stands for higher priority)
Advertisement Interval	Set ad interval	60 sec
Virtual IP	Set Virtual IP	Blank
Authentication Type	Optional: None/Password type	None

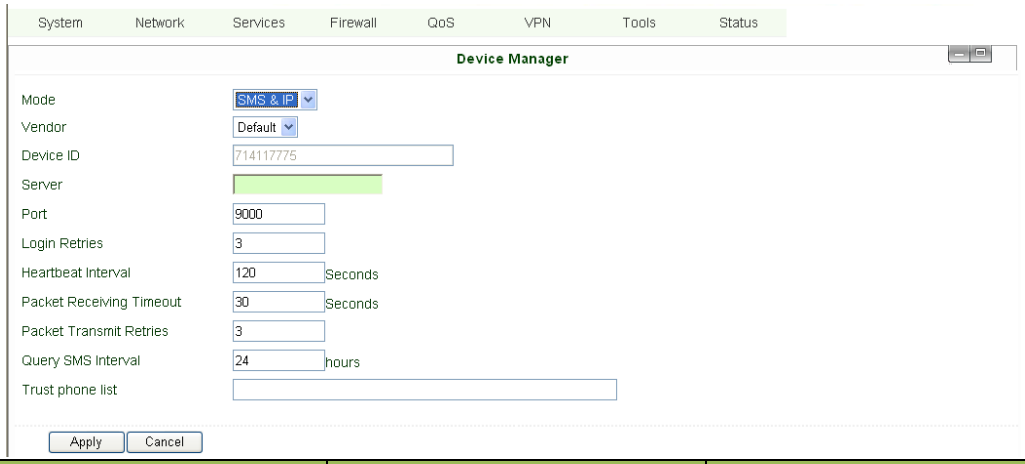
(4) Device Manager



Name	Description	Default
Mode	Disabled/Only SMS/SMS+IP	Disable

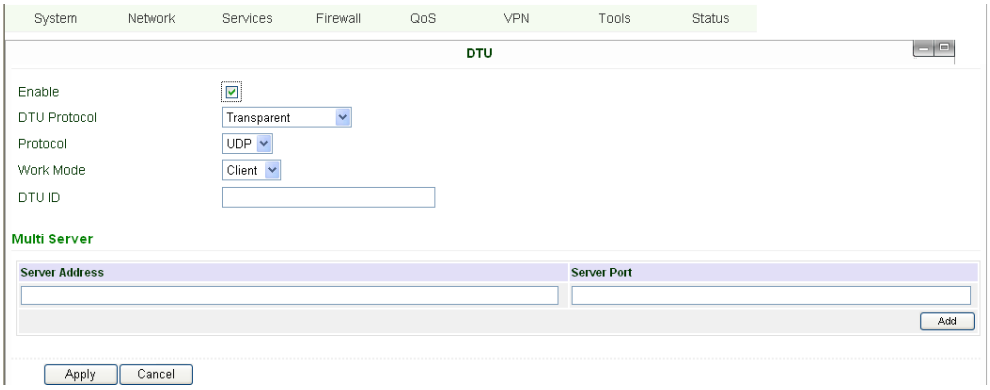


Name	Description	Default
Mode	Only SMS	
Query SMS Interval	Set how long to check SMS	24 hours
Trust Phone List	Add trust Cell Phone List	



Name	Description	Default
Mode	SMS+IP Mode	
Vendor	Set Vendor Name	Default
Device ID	Set Device ID	
Server	Set Device Manager Server IP	
Port	Set Port For DM	9000
Login Retries	Set login retries	3
Heartbeat Interval	Set interval of heartbeat	120
Packet Receiving Timeout	Set packet receiving timeout	30
Packet Transmit Retries	Set packet transmit reties	3
Query SMS Interval	Set how long to check SMS	24
Trust phone list	Set trust cell phone list	

(5) DTU

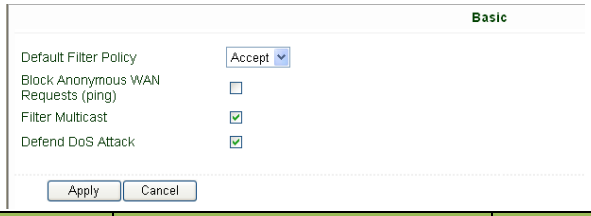


Name	Description	Default
Enable	Click to enable DTU	Disable
DTU Protocol	Set DTU protocol, Please see more in related Quick Guide	Transparent
Protocol	Optional between TCP/UDP	UDP
Work Mode	Set DTU as client or server	Client
DTU ID	Set ID of DTU	Blank
Multi Server	Set the IP address and Port of server to receive data.	Blank

3.1.5 Firewall

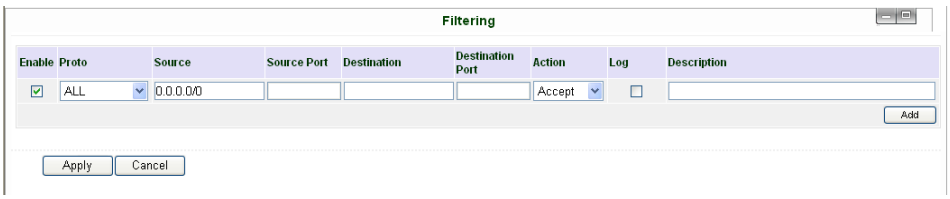
This page is to set parameters concerned with firewall.

(1) Basic Configuration



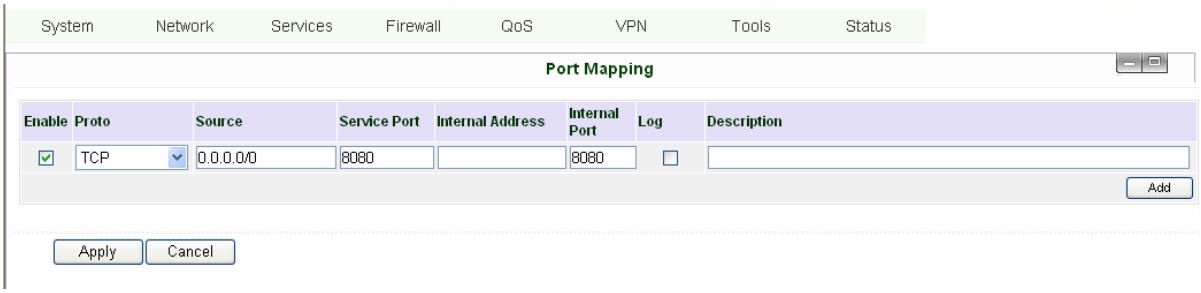
Name	Description	Default
Default Filter Policy	Optional between Accept /Refused	Accept
Block Anonymous WAN Request (ping)	Click to enable filer ping request	Disable
Filter Multicast	Click to enable filter multicast	Enable
Defend DoS Attack	Click to enable Defend DoS Attack	Enable

(2) Filtering



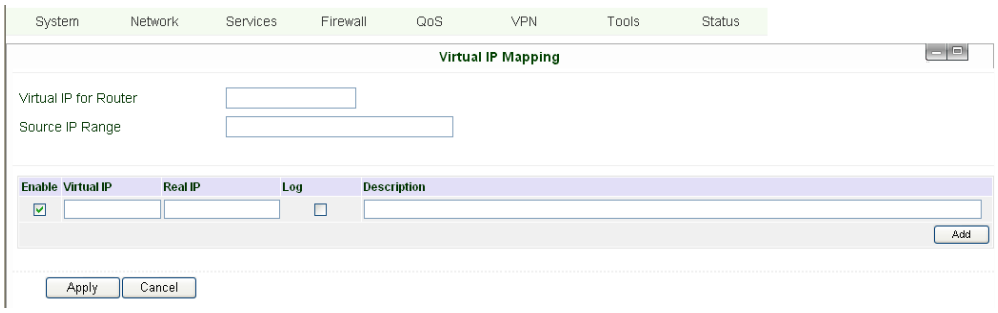
Name	Description	Default
Enable	Click to enable filtering	Blank
Protocol	Optional among TCP/UDP/ICMP	All
Source IP address	Set Source IP address	Blank
Source Port	Set Source Port	Blank
Destination IP	Set destination IP	Blank
Destination Port	Set destination port	Blank
Action	Accept/Deny	Accept
Log	Click to enable login	Disable
Description	Describe your configuration	Blank

(3) Port Mapping



Name	Description	Default
Enable	Click Enable Port Mapping	Disable
Source	To fill with source IP	0.0.0.0/0
Service Port	Fill the port of service	8080
Internal Address	Set the internal IP for mapping	Blank
Internal Port	Set the Port mapping to internal	8080
Log	Click to enable log about port mapping.	Disable
Description	Describe meanings of each mapping	Blank

(4) Virtual IP Mapping

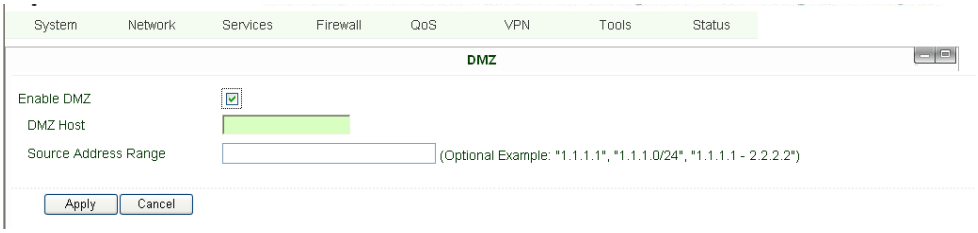


An internal PC's IP can match to a virtual IP, and external network can access to internal PC via this virtual IP address.

Name	Description	Default
Virtual IP for Router	Set Virtual IP for Router	Blank
Source IP Range	Set range of source IP address	Blank
Virtual IP	Set virtual IP	Blank
Real IP	Set real IP	Blank

Log	Enable logging concerned with virtual IP	Disable
Description	Describe this configuration	Blank

(5) DMZ (All Port Mapping)

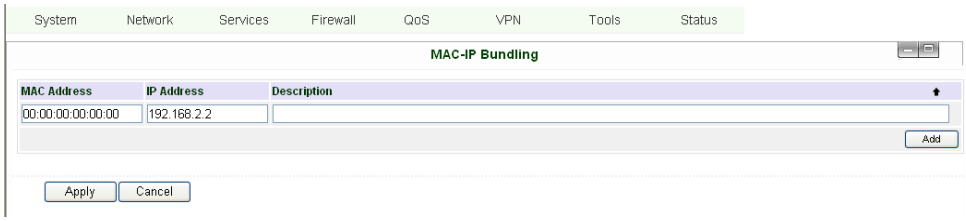


Mapping all the ports and then external PC can get access to all the ports of internal device behind IR600.

Attention: this function cannot help to map the admin port of IR600 (e.g.: 80 TCP) to the device's port.

Name	Description	Default
Enable DMZ	Click to Enable DMZ	Disable
DMZ Host	Set host IP of DMZ	Blank
Source Address Range	Set IP address with restrict IP access	Blank

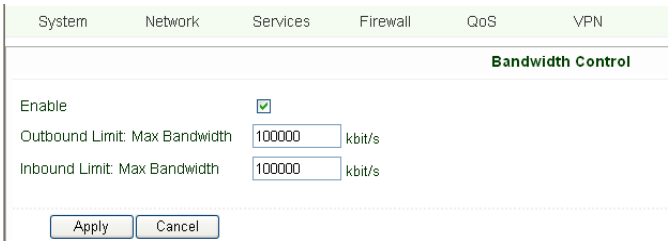
(6) MAC-IP Bundling



When firewall denies all access to the external network, only PC with MAC-IP Bundling can access to external network

Name	Description	Default
MAC Address	Set Bundling Mac address	Blank
IP Address	Set Bundling IP address	192.168.2.2
Description	Describe this configuration	Blank

3.1.6 QoS



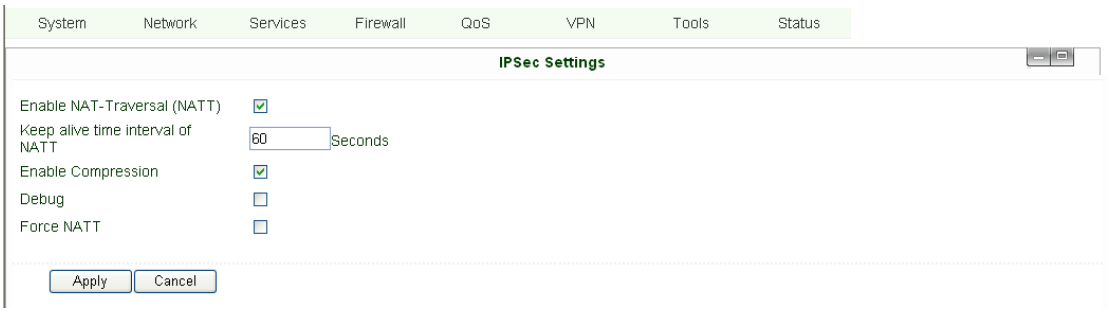
Name	Description	Default
Enable	Click to enable	Disable
Outbound Limit Max Bandwidth	Set the limit speed of out- bound bandwidth	100000kbit/s
Inbound Limit Max Bandwidth	Set the limit speed of inbound bandwidth	100000kbit/s

3.1.7 VPN

This page introduces the parameters set in InRouter 600's Web.

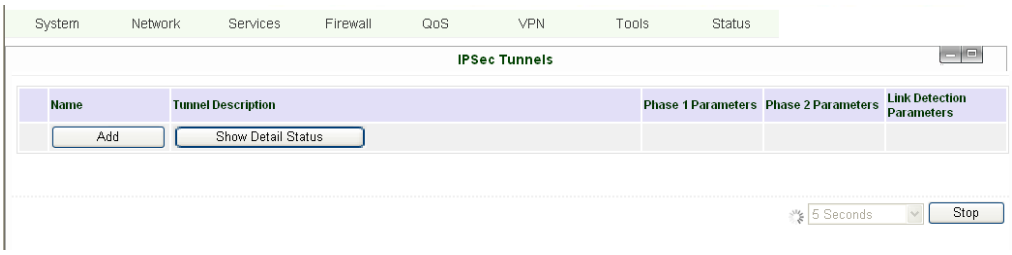
(1) IPSec Settings

To build an IPSec VPN Tunnel, you need first set IPSec properties in this page, then turn to IPSec Tunnels to add your VPN:

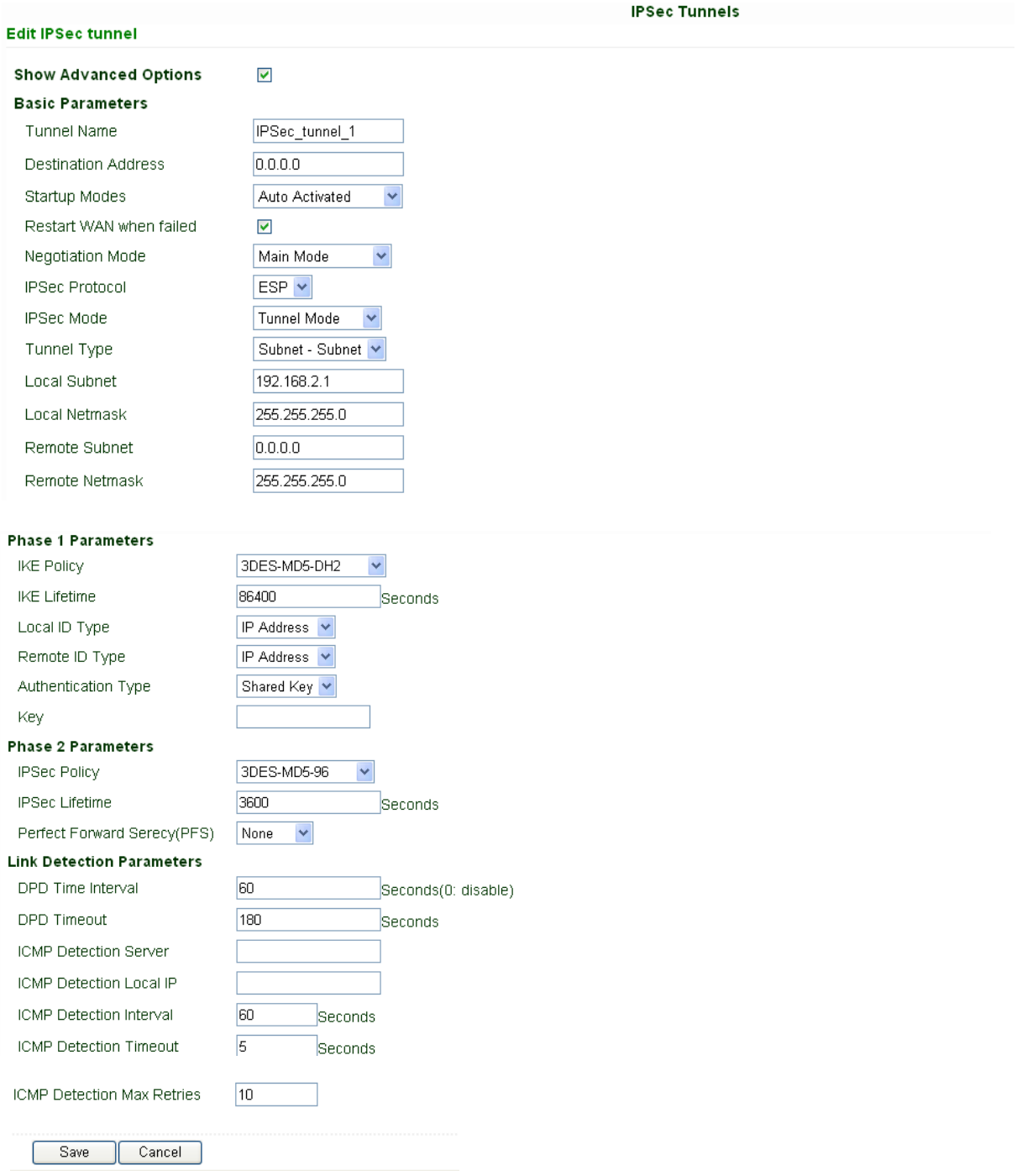


IPSec Settings		
Description: 1. Select to Enable or Disable NATT, normally we need to enable, unless you ensure there is no NAT routers in the network. 2. Select to enable Compression Mode or Debug		
Name	**Description**	**Default**
Enable NAT Transversal (NATT)	Click to enable NATT	Enable
Keep alive time interval of NATT	Set live time for NATT	60 sec
Enable Compression	Click to enable	Enable
Enable Debug	Click to enable	Disable
Force NATT	Click to enable	Disable

(2) IPSec Tunnels



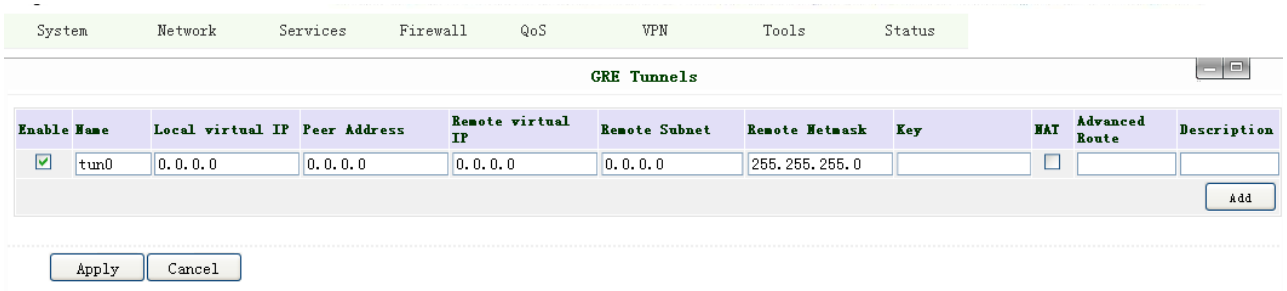
Click "Add" and enter the configuration web:



Name	Description	Default
Show Advanced Options	Click to enable advanced options	Disable
Basic Parameters		
Tunnel Name	To name the tunnel	IPSec_tunnel_1
Destination Address	Set the destination address of IPSec VPN Server	Blank
Startup Mode	Auto Activate/Trigged by Data/Passive/Manually Activated	Enable
Negotiation Mode	Optional: Main Mode or Aggressive Mode	Main Mode
IPSec Mode (Enable Advanced options)	Optional: ESP or AH	ESP
IPSec Mode	Optional: Tunnel Mode or Transport Mode	Tunnel Mode

(Enable Advanced options)		
Tunnel Type	Optional: Host——Host, Host——Subnet, Subnet——Host, Subnet——Subnet	Subnet——Subnet Mode
Local Subnet	Set IPSec Local Protected Subnet	192.168.2.1
Local Subnet Net Mask	Set IPSec Local Protected Subnet Net Mask	255.255.255.0
Remote Subnet Address	Set IPSec Remote Protected Subnet	Blank
Remote Subnet Net Mask	Set IPSec Remote Protected Subnet Net Mask	255.255.255.0
Phase 1 Parameters		
IKE Policy	Optional: 3DES-MD5-96 or AES-MD5-96	3DES-MD5-96
IKE Lifetime	Set IKE 的 Lifetime	86400 sec
Local ID Type	Optional: FQDN, USERFQDN, or IP Address	IP Address
Local ID (Only for FQDN 和 USERFQDN)	Set the ID according to ID type	Blank
Remote ID Type	Optional: FQDN, USERFQDN, or IP Address	IP Address
Remote ID (Only for FQDN and USERFQDN)	Set the ID according to ID type	Blank
Authentication Type	Optional: Shared Key or Certificate	Shared Key
Key (While choosing Shared Key Authentication Type)	Set IPSec VPN Negotiation Key	Blank
Phase 2 Parameters		
IPSec Policy	Optional: 3DES-MD5-96 or AES-MD5-96	3DES-MD5-96
IPSec Lifetime	Set IPSec Lifetime	3600sec
Perfect Forward Secrecy (PFS)	Optional: Disable, GROUP1, GROUP2, GROUP5	Disable ((Enable Advanced options)
Link Detection Parameters (Enable Advanced options)		
DPD Time Interval	Set DPD Time Interval	60sec
DPD Timeout	Set DPD Timeout	180sec
ICMP Detection Server	Set ICMP Detection Server	Blank
ICMP Detection Local IP	Set ICMP Detection Local IP	
ICMP Detection Interval	Set ICMP Detection Interval	30sec
ICMP Detection Timeout	Set ICMP Detection Interval	5sec
ICMP Detection Max Retries	Set ICMP Detection Max Retries	3

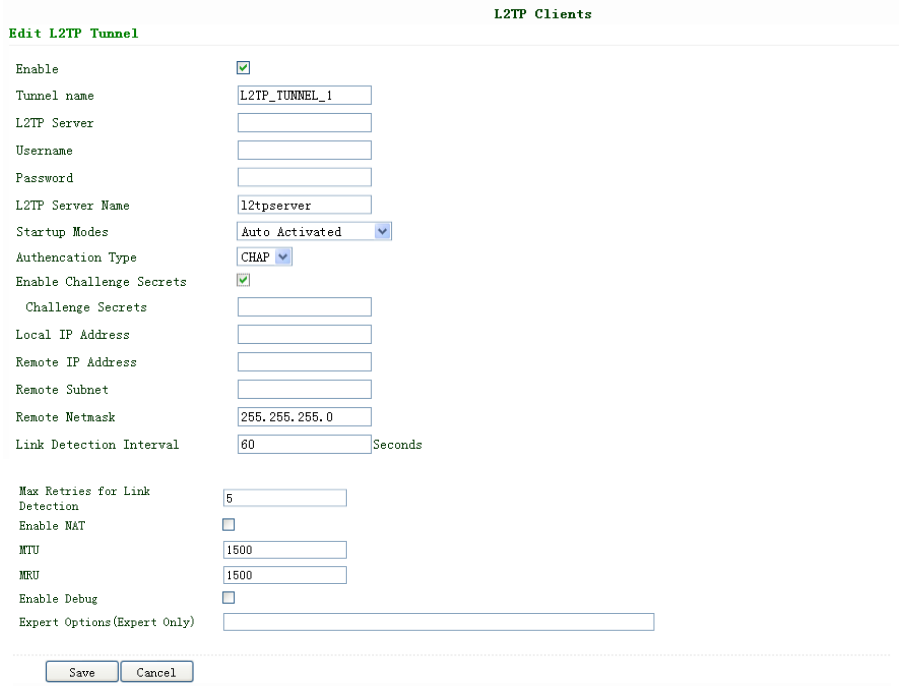
(3) GRE Tunnels



GRE Tunnels		
Name	Description	Default

Enable	Click Enable	Enable
Tunnel Name	Set GRE Tunnel Name	tun0
Local Virtual IP	Set Local Virtual IP	0.0.0.0
Remote Address	Set Remote Address	0.0.0.0
Remote Virtual IP	Set Remote Virtual IP	0.0.0.0
Remote Subnet Address	Set Remote Subnet Address	0.0.0.0
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Key	Set Tunnel Key	Blank
NAT	Click Enable NAT Function	Disable
Description	Add Description	Blank

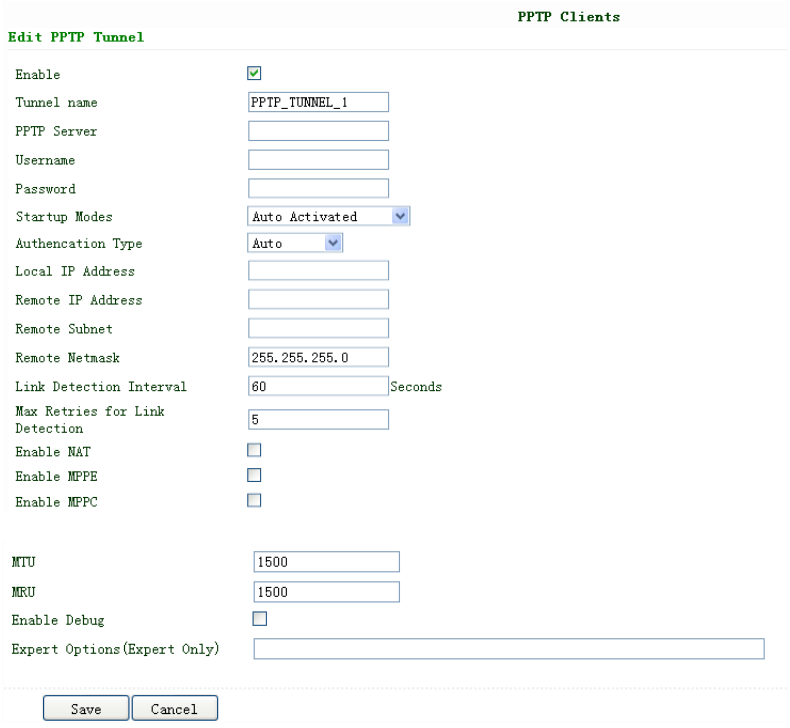
(4) L2TP Clients



Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set Tunnel Name	L2TP_TUNNEL_1
L2TP Server	SetL2TP Server Address	Blank
Username	Set Server Username	Blank
Password	Set Server Password	Blank
Server Name	Set Server Name	l2tpserver
Startup Modes	Set Startup Modes: Auto Activated, Trigged by Data, Manually Activated	Auto Activated
Authencation Type	Set Authencation Type: CHAP, PAP	CHAP
Enable Challenge secrets	Set to enable Challenge secrets	Disable
Local IP Address	Set Local IP Address	Blank
Remote IP Address	Set Remote IP Address	Blank
Remote Subnet	Set Remote Subnet	Blank
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0

Link Detection Interval	Set Link Detection Interval	60
Max Retries for Link Detection	Set Max Retries for Link Detection	5
Enable NAT	Click Enable NAT	Disable
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click Enable Debug Mode	Disable
Expert Options	Set Expert Options	Blank

(5) PPTP Clients



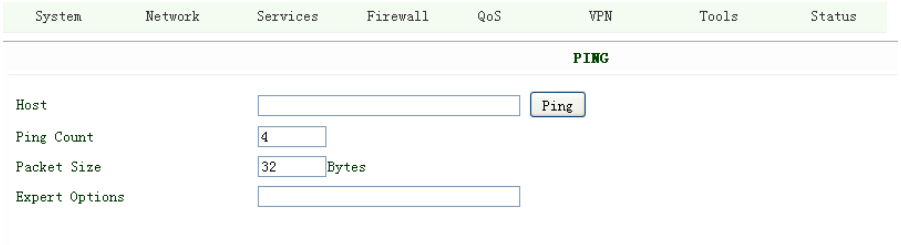
Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set Tunnel Name	PPTP_TUNNEL_1
PPTP Server	Set PPTP Server Address	Blank
Username	Set Server Username	Blank
Password	Set Server's Password	Blank
Startup Mode:	Set Startup Modes: Auto Activated, Trigged by Data, Manually Activated	Auto Activated
Authencation Type	Set Authencation Type: CHAP, PAP, MS-CHAPv1, MS-CHAPv2	Auto
Local IP Address	Set Local IP Address	Blank
Remote IP Address	Set Remote IP Address	Blank
Remote Subnet	Set Remote Subnet	Blank
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Link Detection Interval	Set Link Detection Interval	60
Max Retries for Link Detection	Set Max Retries for Link Detection	5
Enable NAT	Click Enable NAT	Blank

Enable MPPE	Click Enable MPPE	Blank
Enable MPPC	Click Enable MPPC	Blank
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click Enable Debug Mode	Blank
Expert Options	For InHand R&D only	Blank

3.1.8 Tools

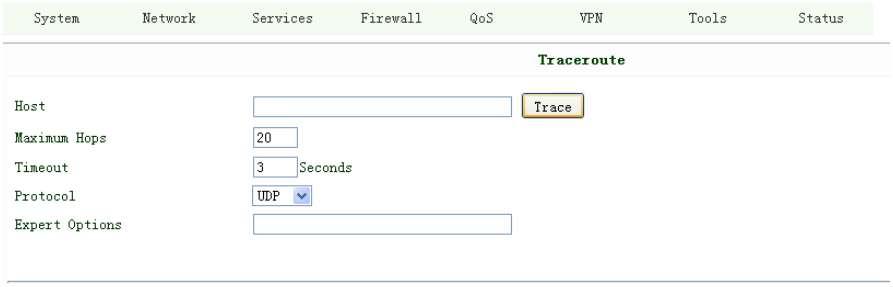
Tools contain PING Detection, Route Trace, Link Speed Test and etc.

(1) PING



Name	Description	Default
Host	Destination for PING	Blank
Ping Count	Set PING Counts	4 times
Packet Size	Set PING Packet Size	32 Bytes
Expert Options	Advanced parameters	Blank

(2) Trace Route



Name	Description	Default
Host	Destination for Trace Route	Blank
Max Hops	Set Max Hops	20
Time Out	Set Time Out	3 sec
Protocol	Optional: ICMP/UDP	UDP
Expert Options	Advanced parameters	Blank

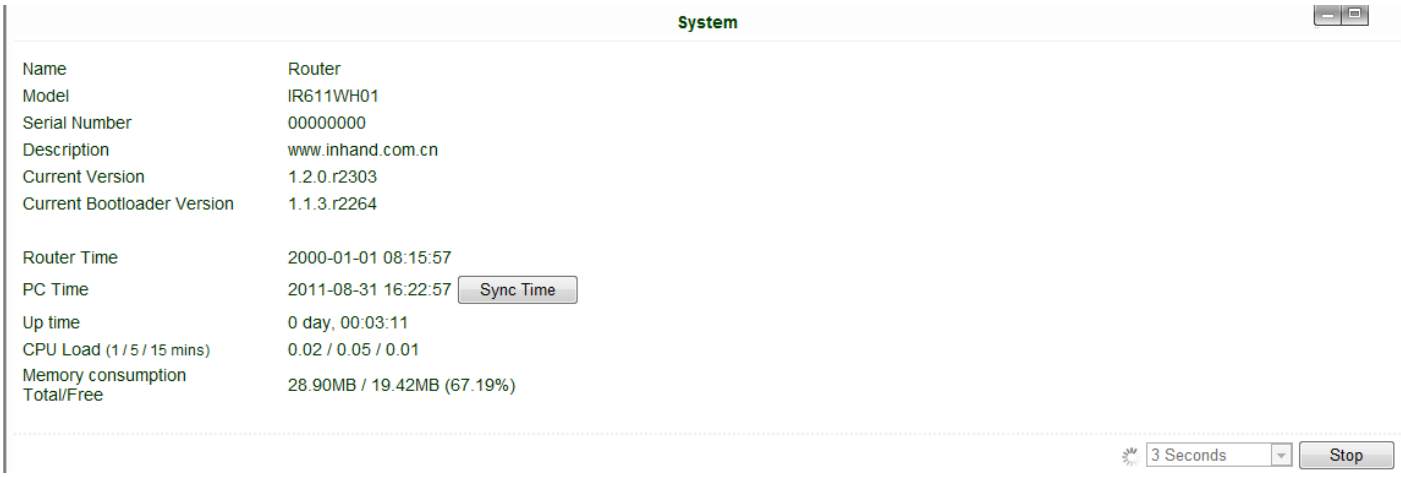
(3) Link Speed Test

Test link speed via unload or download

3.1.9 Status

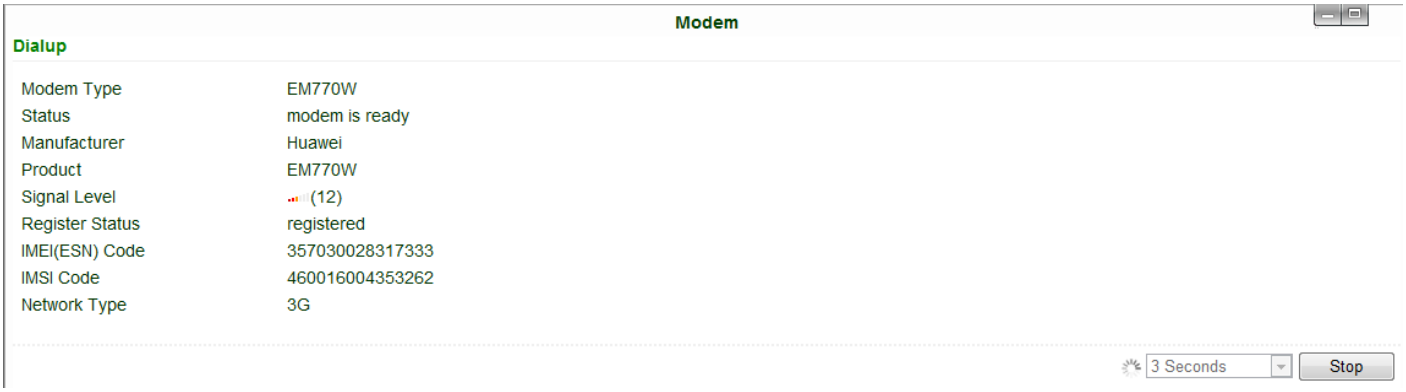
Status contains System, Modem, Network Connections, Route Table, Device List and Log.

(1) System Status



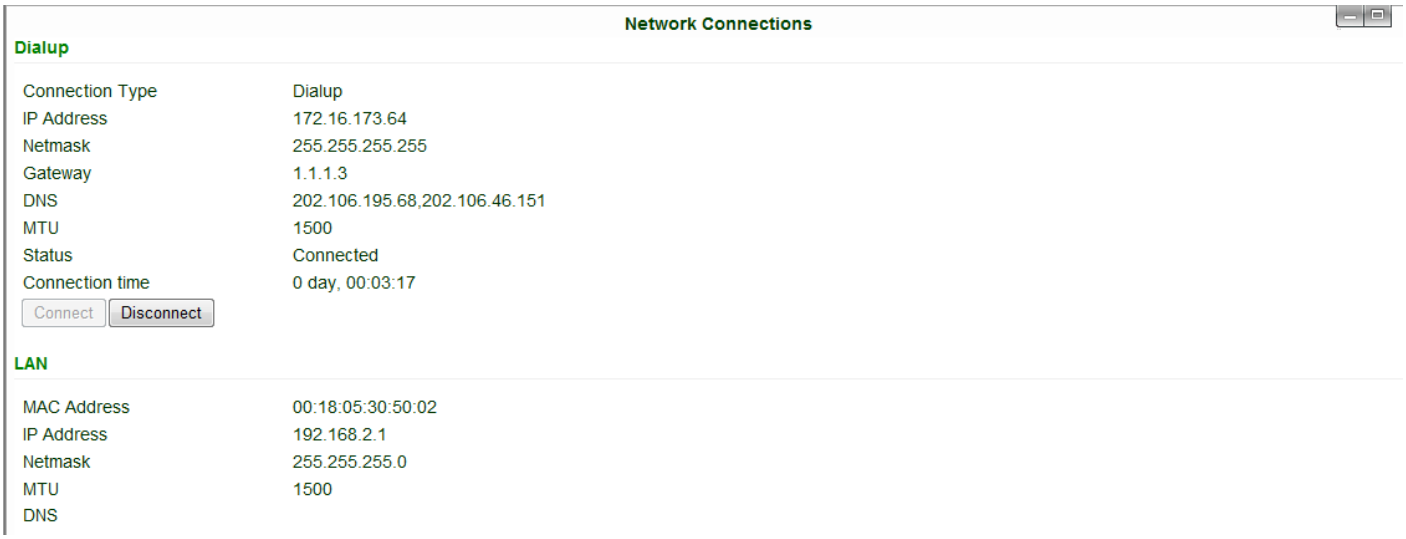
This page shows the status of system, including Name, Model Type, Current Version and etc.

(2) Modem Status



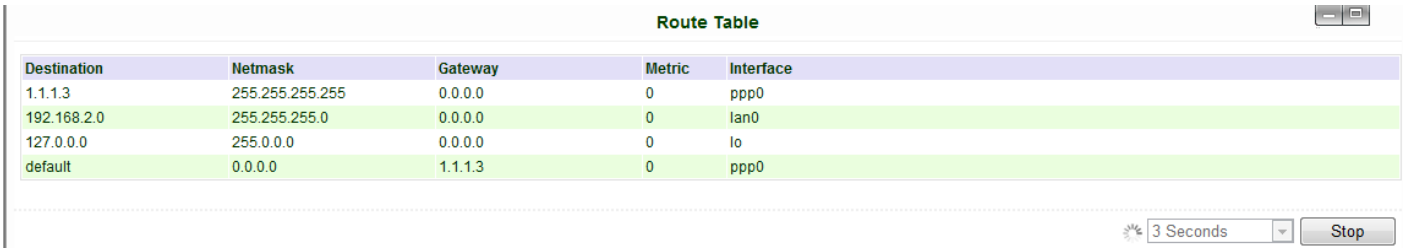
This page shows the status of Modem, including the signal level.

(3) Network Connections



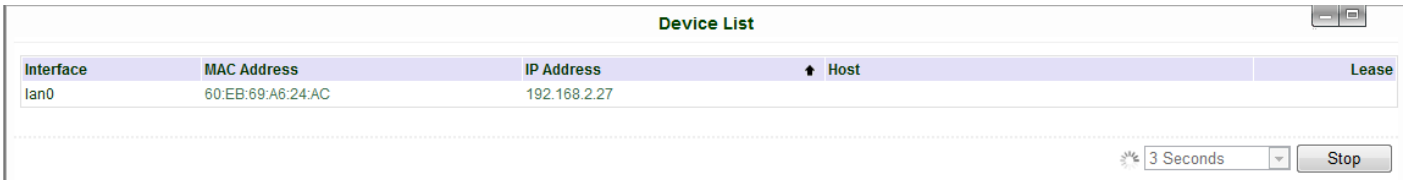
This page shows the network connections via WAN or LAN

(4) Route Table



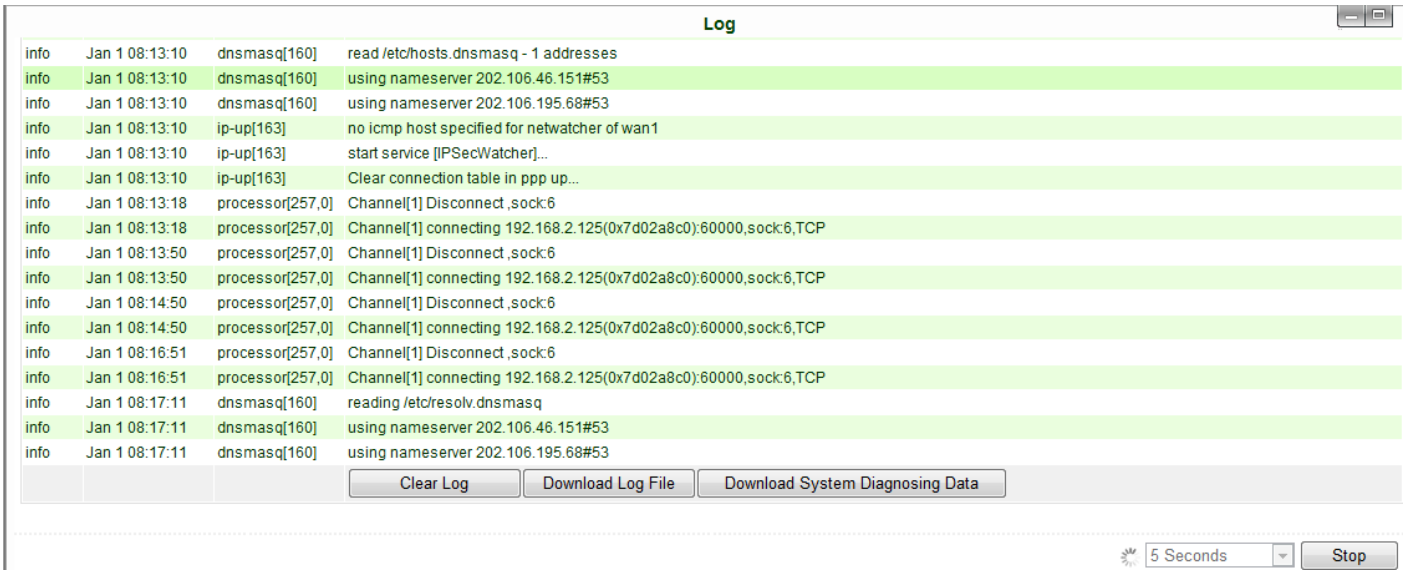
This page shows the route table of IR600.

(5) Device List



This page shows the devices linked with IR600.

(6) Log


Log
info Jan 1 08:13:10 dnsmasq[160] read /etc/hosts.dnsmasq - 1 addresses
info Jan 1 08:13:10 dnsmasq[160] using nameserver 202.106.46.151#53
info Jan 1 08:13:10 dnsmasq[160] using nameserver 202.106.195.68#53
info Jan 1 08:13:10 ip-up[163] no icmp host specified for netwatcher of wan1
info Jan 1 08:13:10 ip-up[163] start service [IPSecWatcher]...
info Jan 1 08:13:10 ip-up[163] Clear connection table in ppp up...
info Jan 1 08:13:18 processor[257,0] Channel[1] Disconnect ,sock:6
info Jan 1 08:13:18 processor[257,0] Channel[1] connecting 192.168.2.125(0x7d02a8c0):60000,sock:6,TCP
info Jan 1 08:13:50 processor[257,0] Channel[1] Disconnect ,sock:6
info Jan 1 08:13:50 processor[257,0] Channel[1] connecting 192.168.2.125(0x7d02a8c0):60000,sock:6,TCP
info Jan 1 08:14:50 processor[257,0] Channel[1] Disconnect ,sock:6
info Jan 1 08:14:50 processor[257,0] Channel[1] connecting 192.168.2.125(0x7d02a8c0):60000,sock:6,TCP
info Jan 1 08:16:51 processor[257,0] Channel[1] Disconnect ,sock:6
info Jan 1 08:16:51 processor[257,0] Channel[1] connecting 192.168.2.125(0x7d02a8c0):60000,sock:6,TCP
info Jan 1 08:17:11 dnsmasq[160] reading /etc/resolv.dnsmasq
info Jan 1 08:17:11 dnsmasq[160] using nameserver 202.106.46.151#53
info Jan 1 08:17:11 dnsmasq[160] using nameserver 202.106.195.68#53
Clear Log
Download Log File
Download System Diagnosing Data
5 Seconds
Stop

This page shows the log of system, including download log file.

For some situation when there're some problems that can't be diagnosed at the moment, you'll be asked to provide the diagnose log to InHand engineers, you can click "Download System Diagnosing Data" then send the diagnose log to us.

3.2 Support

In case you have problems with the installation and use, please address them to us by e-mail: support@inhandnetworks.com.

Copyright © 2011 InHand Networks, All rights reserved.

Tel: 86-10-64391099-8022
Fax: 86-10-84170089
Address: Wangjing Science Park, Road Lizezhonger, Chaoyang District, Beijing, P. R. C, 100102
Website: http://www.inhandnetworks.com
Email: info@inhandnetworks.com

Subject to alterations without notice.